



LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Yrityksen X hallinnollisen turvallisuuden kehittäminen Katakriin avulla

Kälviäinen, Ilmari

2015 Laurea

Laurea-ammattikorkeakoulu

Yrityksen X hallinnollisen turvallisuuden
kehittäminen Katakryn avulla

Kälviäinen Ilmari
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Marraskuu, 2015

Kälviäinen Ilmari

Yrityksen X hallinnollisen turvallisuuden kehittäminen Katakriin avulla

Vuosi 2015 Sivumäärä 96

Tämän opinnäytetyön tavoitteena oli kartoittaa yrityksen X hallinnollisen turvallisuuden nykytila ja taso. Saatujen arviointitulosten perusteella oli tarkoitus luoda kehittämis ehdotus turvallisuuden parantamiseksi. Kartoitus toteutettiin Kansallisen turvallisuusauditointikriteeristä tehtyjen versioiden II ja 2015 avulla. Tarkoituksena oli myös selvittää Katakriin soveltuvuus kohdeorganisaation kokonaisturvallisuuden auditointi- ja kehittämisvälineeksi. Katakriin mukainen auditointi ei ollut virallinen eikä pakollinen ja prosessia ei toteutettu loppuun saakka. Turvallisuusauditointi toteutettiin Katakriin hallinnollisen turvallisuuden pääosa-alueesta. Poikkeamakäsittelyn vertailuarvoiksi asetettiin Katakri II:n osalta Elinkeinoelämän keskusliiton (EK:n) laatima suositustaso ja Katakri 2015 osalta kaikille vaatimustasona pidetty perustaso.

Opinnäytetyö oli laadullinen tutkimus, jossa käytettiin kvalitatiivisena tutkimuslajina hermeneuttista menetelmää. Tutkimuksen primäärisinä tiedonkeruumenetelminä käytettiin dokumenttianalyysejä, strukturoituja kyselyjä ja teemahaastatteluja. Sekundaarisina tiedonkeruumenetelminä käytettiin kohdeorganisaation esimiehille suunnattua Katakrista johdettua kvantitatiivista turvallisuuskyselyä sekä koko auditointiprosessin ajan havainnointia.

Tämä tutkimus alkaa tavoitteen määrittelystä ja tutkimuskohteen toimintaympäristön esittelystä. Alkutiedoista siirrytään teoreettiseen viitekehykseen ja aihealueeseen liittyvien keskeisiin määritelmiin. Teoreettisten lähtökohtien jälkeen esitellään itse auditointiväline Katakri sekä suoritettu auditoinnin toteutus. Auditointitulokset ja havainnot nykytilasta esitetään sekä Katakriin mukaisina poikkeama-arvioina että analyyseinä. Tuloksista havaittujen puutteiden mukaan esitetään kohdeorganisaatiolle analyysejä hallinnollisen turvallisuuden nykytilasta ja tasosta sekä kehittämis ehdotus kokonaisturvallisuuden parantamiseksi. Kohdeorganisaatio voi käyttää tuotettua kehittämis ehdotusta hallinnollisen turvallisuutensa eri osa-alueiden parantamiseen ja lisätä ehdotuksen mukaisilla kehitystoimilla yrityksensä kokonaisturvallisuutta.

Turvallisuusauditoinnin arviointitulos osoitti, että kohdeorganisaation hallinnollinen turvallisuus ei tavoittanut asetettua, kriteeristön mukaista, tasovaatimusta. Kriteeristövaatimukset täyttyivät ainoastaan 11 %:n osalta. Auditoinnissa tehtyjen havaintojen perusteella vaatimaton tulos johtuu siitä, että kohdeorganisaation turvallisuustoiminnan painopiste oli suunnattu pelkästään työ-, henkilö- ja tilaturvallisuuden osa-alueille. Siten saatu poikkeamien kokonaistulos hyvin hoidettujen osa-alueiden näkökulmasta katsottuna oli hyvin ankara. Organisaation turvallisuudessa puutteellisimmiksi osiksi osoittautuivat riskien mukainen kokonaisturvallisuuden suunnitelmallinen ja tavoitteellinen toiminta, tietohallinnon ulkoistuksen hallintaan liittyvät varmistukset, tietoturvallisuuden huomioiminen ja varautumissuunnittelu.

Toteutettu turvallisuusauditointi synnytti ideoita ja avasi kokonaisturvallisuuden kenttää haastateltavien keskuudessa niin hyvin, että moni teki jo auditoinnin aikana huomioita eniten kehittämistä tarvitsevista kohteista. Jos turvallisuuden kehittämistä päätetään jatkaa ja auditointia laajentaa toteuttamalla esimerkiksi turvallisuusauditoinnissa rajauksen ulkopuolelle jääneillä osa-alueilla, tässä työssä tehtyjen havaintojen ja huomioiden mukaan, kaikesta työläydestään huolimatta Katakri soveltuu turvallisuuskehittämisen auditointivälineeksi hyvin.

Asiasanat: Turvallisuusjohtamisjärjestelmä, turvallisuusjohtaminen, riskienhallinta, auditointi, Kansallinen turvallisuusauditointikriteeristö

Kälviäinen Ilmari

The Development of a Company's Administrative Security by KATAKRI

Year	2015	Pages	96
------	------	-------	----

The aim of this thesis was to survey the current state and the level of the target organization's administrative security. Based on the evaluation of the results this thesis was to create the development proposal to improve the security. The survey was carried out by the National Security Auditing Criteria (KATAKRI) in II versions and also the latest version 2015. The second purpose was to determine the suitability of KATAKRI development tool for the target organization's overall security. According to KATAKRI the audit was neither official nor mandatory and the process was not carried out until the end. The audit of security was carried out by KATAKRI's main area of the administrative security. As a benchmark it was set the level of recommendation of Confederation of Finnish industries (EK) for KATAKRI II and the basic level according to all standards for KATAKRI 2015.

The thesis was a qualitative research, using hermeneutical method. As the primary data collection methods in this thesis were used documentary analysis, structured questionnaires and thematic interviews. As the secondary data collection methods quantitative security survey and structured interviews were used and directed to the target organization for managers. In addition, throughout the audit period observation was used, as a method.

This thesis begins by defining the objective and the presentation of research environment. It will then go on to the theoretical framework and the definitions of the key themes. After the theoretical starting point the audit tool KATAKRI II and 2015 are presented, as well as the implementation of the audit. The audit results and observations of the current state are shown as well as in line with the offset estimates and analyses. According to the problems detected, the results of the current state of the target organization and the level of administrative security analysis are presented, as well as a development proposal to improve the overall security. The development proposal is provided in order that the target organization can use this report to improve administrative security and to increase development efforts in the company's overall security.

The security audit evaluation results showed that the object of the organization's administrative security did not reach the required level. In this case only 11 % of the criteria requirements was fulfilled. The reason for the modest result of the audit was that the target organization's operational focus of security was exclusively directed at employment, social security and property security areas. KATAKRI does not take into account the matters that have been done well. Therefore, the evaluation of the results of total security was very difficult. In addition, a number of problems were found in the security audit. One problem was that any security plans were not implemented by risks analysis, another major problem was the management of Information Technology. The organization did not have backups or did not have any plans for data security.

This security audit provoked ideas and opened up new prospects in the total security field among the interviewees. During the audit observations many interviewees found out the most needed development targets. If the development of the security will be adopted to continue and expand the audit, for example, by carrying out security audits in the areas which have not yet been dealt with at all, taking into account the observation made in this study, KATAKRI audit tool is a well suitable security development tool.

Keywords: Security management system, security management, risk management, auditing, National Security Auditing Criteria (KATAKRI)

Sisällys

1	Johdanto.....	7
2	Tutkimuksen lähtökohdat.....	8
2.1	Alkuasetelma ja tavoitteiden määrittäminen.....	8
2.2	Kehittämismallin valinta ja aiheen rajaaminen.....	8
2.3	Toimintaympäristö, kohdeorganisaatio ja sidosryhmät.....	10
2.4	Aiemmat tutkimukset.....	10
3	Tutkimuksen teoreettinen viitekehys.....	11
3.1	Teoreettinen pohdiskelu, tutkimusongelma ja -kysymykset.....	11
3.2	Keskeiset määritelmät ja käsitteet.....	14
3.3	Onnettomuuksien syntyminen ja inhimilliset tekijät.....	14
3.4	Riskienhallinta.....	19
3.5	Turvallisuusjohtaminen.....	21
3.6	Turvallisuusjohtamisjärjestelmä.....	25
3.7	Auditointi.....	28
4	Kansallinen turvallisuusauditointikriteeristö.....	30
4.1	Katakri II.....	30
4.2	Katakri 2015.....	31
4.3	Auditointiohjelma ja toteutus.....	32
5	Empiirinen tutkimusasetelma.....	34
5.1	Tutkimusote ja toimintatavat.....	35
5.2	Tiedonkeruu- ja analysointimenetelmät.....	36
5.2.1	Dokumenttianalyysi.....	36
5.2.2	Haastattelu.....	37
5.2.3	Kysely.....	38
5.2.4	Havainnointi.....	40
5.2.5	Tietoaineiston analysointi.....	41
6	Auditointitulokset Katakriin mukaan.....	41
6.1	Auditoinnista saadut arviointitulokset.....	43
6.2	Turvallisuuden nykytilan ja tason arviointi.....	45
6.2.1	Turvallisuustoiminnan toteuttamisen ongelma.....	45
6.2.2	Turvallisuudesta vastaavien työnkuvat, vastuut ja organisointi.....	46
6.2.3	Turvallisuusorganisaatio ja tilannekuva.....	47
6.2.4	Riskienhallinta.....	47
6.2.5	Turvallisuudelle asetetut tavoitteet.....	48
6.2.6	Tietohallinto.....	48
7	Katakriin mukaan tehdyt kehittämissuositukset.....	49
7.1	Turvallisuuden organisointi ja vuosikello.....	51
7.2	Ylin johto.....	53

7.2.1	Yrityksen johdon strategiset linjaukset ja päätökset	53
7.2.2	Yrityksen johdon tekemät vastuunjaot, toimivaltuudet ja resurssit	54
7.2.3	Turvallisuuden tilannekuva ja toiminnan taso	55
7.2.4	Yrityksen toiminnan kannalta tärkeät suojattavat kohteet.....	55
7.3	Turvallisuusjohtaminen	56
7.3.1	Yrityksen turvallisuuspolitiikka	56
7.3.2	Riskienhallintaprosessi	56
7.3.3	Turvallisuustavoitteiden määrittely	57
7.3.4	Kokonaisturvallisuuden suunnitelmallinen hallinta	57
7.3.5	Turvallisuuspoikkeamatilanteet	57
7.3.6	Kehittämisen vaikutusanalyysit	58
7.4	Henkilöstöhallinto.....	58
7.4.1	Tehtäväkuvaukset	58
7.4.2	Asiakirjahallinto ja luokitukset	59
7.4.3	Lainsäädännön seuranta	59
7.4.4	Turvallisuusdokumentaatioiden hallinta	60
7.5	Tietohallinto	60
7.5.1	Tietohallinnon toimintasuunnitelma ja tietoturvapoliittika.....	60
7.5.2	Ulkoistetun palveluntuottajan hallinta.....	61
7.5.3	Tietohallinnon käyttöoikeuksien hallinta	62
7.5.4	Tietoturvaohjeistukset	62
7.5.5	Tietoturvapoikkeamien hallinta	62
7.6	Linjaorganisaatio	63
7.6.1	Perehdytys-, koulutus-, seuranta-, valvonta- ja tiedottamisvastuu.....	63
7.6.2	Poikkeamatilanteisiin varautuminen.....	64
7.7	Asiakkuudenhallinnassa turvallisuusnäkökulman parantaminen	64
8	Johtopäätökset	67
8.1	Hallinnollisen turvallisuuden auditointi	67
8.2	Katakrin soveltuvuus auditointivälineeksi	68
8.3	Oman työn arviointi.....	69
	Lähteet	70
	Kuviot	73
	Taulukot	74
	Liitteet.....	75

1 Johdanto

Tämän opinnäytetyön kohteena oli suomalainen yritys, jossa oli todettu tarve kehittää turvallisuutta. Viimeisten vuosien aikana yrityksessä oli parannettu työn turvallista suorittamista ja kiinnitetty erityistä huomiota turvallisen palvelun tuottamiseen. Saavutettujen hyvien tulosten innoittamina yrityksessä herättiin kehittämään turvallisuutta myös laajemmin. Tämän opinnäytetyön tavoitteena oli jatkaa aloitettua hyvää työtä ja löytää kohdeyrityksen turvallisuudesta ja turvallisuusjohtamisesta kokonaisvaltaisesti kehitettäviä asioita. Tarkoituksena oli saada aikaan kehittämis ehdotus, jonka mukaan voi suoraan toteuttaa kehittämistoimia ja myös tulevaisuudessa luoda suunnitelmia turvallisuuden parantamiseksi.

Kehittämiskohteita voidaan nimetä ja tehdä arvioita vasta, kun löydetään ja tunnistetaan turvallisuudesta ja turvallisuusjohtamisesta merkittäviä puutteita tai epäkohtia. Tätä tutkimusta ohjaa ajatus, että kaikki yrityksessä toteutuneet uhat, vaarat, vahingot ja häiriöt johtuvat yrityksen turvallisuusjohtamisen puutteista ja epäkohdista. Ajatus kumpuaa Kerkon (2001, 14) esittämästä tutkimustuloksesta, jonka mukaan yrityksessä tapahtuvat toimintahäiriöt ja onnettomuudet johtuvat 90 prosenttisesti inhimillisistä tekijöistä ja johtamisjärjestelmässä esiintyvistä puutteista. Vaikka kaikkeen ei voi varautua, niin kaikkea voi kuitenkin kehittää, erityisesti yrityksen hallinnollista turvallisuutta ja turvallisuusjohtamista.

Tutkimustavoitteeseen pääsemiseksi toteutettiin kohdeyrityksessä turvallisuusauditointi. Auditoinnin tarkoituksena oli selvittää yrityksen turvallisuuden nykytilanne ja taso. Auditointivälineeksi valikoitui kansallinen turvallisuusauditointikriteeristö Katakri. Auditoinnin toteuttamiseksi tämä työ rajattiin käsittämään Katakriin hallinnollisen turvallisuuden osa-alueet. Koska Katakreja on julkaistu useita, otettiin tätä suoritettua auditointia varten käyttöön Katakriin II versio ja myös uusiin 2015 versio, jotka kriteeristön osalta yhdistettiin yhdeksi vertailussa käytettäväksi auditointikriteeristöksi. Katakri II:n vertailutasoksi valittiin elinkeinoelämän keskusliiton (EK:n) suositustaso. Katakri 2015 versiosta otettiin myös auditointiin mukaan turvallisuusjohtamisen osa-alueen hallinnollisen turvallisuuden osat, joita uudessa kriteeristössä on kuvattu vähimmäiseksi täytettäväksi perustasoksi. (Katakri II 2011, 3; Katakri 2015, 2.)

Tämän työn toinen tarkoitus oli selvittää Katakriin soveltuvuutta ja käyttökelpoisuutta kohdeyrityksen auditoinnin ja kokonaisturvallisuuden kehittämisen välineenä. Vaikka Katakrit ovat suunniteltuja viranomaiskäyttöön, voi niitä silti vapaasti käyttää hyväksi yritysten omaehtoisessa turvallisuustyössä. Esimerkiksi Katakri II versio on monipuolinen auditoinnin perustyökalu, jossa EK:n suositustason lisäksi on määritelty myös kolme vaativampaa turvallisuustasoa. Yrityksen turvallisuutta voi siten parantaa ja kehittää Katakriin avulla monin eri tavoin. Laaditulla jatkuvan kehittämisen suunnitelmalla voi yrityksessä edetä esimerkiksi vaatimustaso kerrallaan sekä nykytasoa ja edistymistä säännöllisesti arvioida sisäisillä auditoinneilla.

2 Tutkimuksen lähtökohdat

Tässä luvussa kerrotaan, mistä lähtökohdista tämä opinnäytetyön aihe ja tavoitteet saivat alkunsa. Samalla esitellään työssä käsiteltävää kohdeorganisaatiota niin paljon kuin se on vain anonymisti mahdollista. Tässä luvussa kuvataan myös esiselvityksessä saatujen vastausten ja kohdeyrityksestä tehtyjen alkuhavaintojen mukaan lähtökohtatilannetta ja toimintaympäristöä, jossa kehittämistyö määriteltiin, suunniteltiin, auditointiosuus toteutettiin.

2.1 Alkuasetelma ja tavoitteiden määrittäminen

Kohdeyrityksestä tehtyjen esiselvityksen perusteella muodostui yleiskuva yrityksen tarpeesta toteuttaa kokonaisturvallisuuden kehittämisprojekti. Yrityksen tärkeimmäksi kohteeksi valikoitui turvallisuusjohtamisen kokonaistarkastelu turvallisuuden kehittämisenäkökulmasta. Jatkoselvityksissä tehdyt arviot kohteen yleistilanteesta ja esitetty turvallisuusasioiden kehittämiseen tarvittava toimintavalmius vahvistivat käsitystä, että kehittämistyö oli myös toteuttamiskelpoinen ja realistinen. Kohdeyrityksen tarkoituksena oli jatkaa tämän selvitystyön pohjalta turvallisuuden parantamista ja jatkokehittämistyötä. Työn tavoitteeksi muotoutui siten saada aikaan sellainen kattava selvitys, jota voidaan käyttää yrityksessä suoraan kehittämis- ja projektisuunnitelmien tukena tai määrittäessä uusia tavoitteina.

Ajatuksena oli myös lähitulevaisuudessa jatkaa turvallisuuden kehittämistyötä auditoimalla myöhemmin, nyt tästä työstä pois rajatuilla osa-alueilla, kuten henkilöstö- ja tietoturvallisuudella sekä fyysisellä turvallisuudella. Suunnitelman tarkoitus on ottaa käyttöön yrityksen kokonaisvaltainen riskienhallinta sekä kaikkien turvallisuusjohtamisjärjestelmään kuuluvien osa-alueiden lisäksi luoda kokonaisturvallisuudelle jatkuvan kehittämisen toimintamalli.

2.2 Kehittämismallin valinta ja aiheen rajaaminen

Jotta voitaisiin tunnistaa ja löytää kehittämistä vaativat kohteet, on ensin selvittävä jollakin yleisesti hyväksyttävällä menetelmällä vallitsevaa nykytilannetta. Hyväksyttävä menetelmä tulee olla sellainen, jolla voidaan puolueettomasti osoittaa, että kehittämiskohteita ei ole valittu sattumanvaraisesti tai jollakin muulla henkilöön tai tunteisiin liittyvällä tai muuhun tilanteeseen sopivalla tavalla. Nykytilanne on siten saatava kartoitettua luotettavasti, systemaattisesti ja yhdenvertaisesti juuri kartoittamista varten soveltuvalla menetelmällä. Valittavalla menetelmällä on myös oltava jokin vertailuväline, esimerkiksi kysymyslista tai jo olemassa oleva vaatimuskriteeristö, jota vasten voidaan saatuja tuloksia ja havaintoja verrata.

Edellä mainittujen esiselvitysten ja keskusteluiden perusteella päädyttiin tilanteeseen soveltuvimmasta kehittämistyön toteutus- ja menettelytapamallista. Tärkeimmäksi tavoitteeksi

muodostui kohdeorganisaation kokonaisturvallisuuden ja turvallisuusjohtamisen nykytilan selvittäminen, jotta saataisiin tietoa puutteista ja kehittämistarpeista. Kohdeyrityksen turvallisuustason todentamisen tarkastusvälineeksi valittiin kansallinen turvallisuusauditointikriteeristö Katakri. Nykytilan kartoitus päätettiin toteuttaa sisäisellä esiauditoinilla.

Kartoitusmalliksi valittiin esiauditointi, koska Katakriin mukaan varsinainen auditointiprosessi toteutettuna tarkoittaisi, että auditointitapahtumia jatkettaisiin kunnes kaikkien osa-alueiden kriteeristöt olisivat kohdeorganisaation taholta saatu täytettyä (Katakri II 2011, 4). Esiauditointiprosessin toteutus on perusteltua myös siksi, että kohdeorganisaation turvallisuutta ei tarvitse tarkastella kriittisesti, koska se ei ole turvallisuuskriittinen organisaatio eikä sille ole asetettu mitään viranomaisvaatimuksia. (Reiman & Oedewald 2008, 17.)

Opinnäytetyössä tehtävä kartoitus rajattiin käsittämään ainoastaan Katakri II:n hallinnollisen turvallisuuden ja turvallisuusjohtamisen osa-alueet (A100 - A900), EK:n suositustasovaatimusten mukaisesti (Katakri II 2011, 1). Katakri 2015 versiosta otettiin mukaan Turvallisuusjohtamisen (T), osa-alueesta Hallinnollisen turvallisuuden osat, joita on uudessa kriteeristössä kuvattu täytettäväksi vähimmäistasoksi ilman tasoluokitusta eli perustasoksi, jonka taso on yrityksen aina täytettävä. Auditointi toteutetaan esiauditointina, joka tarkoittaa, että toteutus tapahtuu vain yhtenä kertaluontoisena tarkastustapahtumana. (Katakri 2015, 2.)

Rajausta perustellaan sekä kohdeorganisaation toiveella että auditointityön laajuuden hallittavuudella. Ensimmäinen auditointi, joka kohdeyritykselle tämän työn osalta suoritettiin, haluttiin kohdentuvan juuri ylätason turvallisuustoiminnan nykytilan selvittämiseen. Rajauksen tarkoitus ja tavoite oli varmistaa, että kaikki toiminnallisesti tärkeät ja merkittävät turvallisuuspuutteet tulisi ensin tunnistaa sekä sitten korjata kuntoon, ennen kuin varsinaiseen turvallisuustoiminnan kokonaiskehittämiseen on mahdollista siirtyä. Auditoinnin toteuttamiseksi yhdistettiin rajauksen mukaisesti kaikki hallinnollisen turvallisuuden, Katakri II:n A ja Katakri 2015:a T osa-alueet yhdeksi vertailussa käytettäväksi auditointikriteeristöksi. Yhdistämistä perustellaan sillä, että näin menetellen saadaan hyödynnettyä uuden ja vanhan kriteeristön kaikkia vaatimuksia sekä laajennettua auditointia kokonaisvaltaisemmaksi tarkasteluksi.

Opinnäytetyön ulkopuolelle jäivät siten Katakri II:n (osa-alueet P, F ja I) eli henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuuden osa-alueet (Katakri II 2011, 1). Tämän työn ulkopuolella jäivät pois Katakri 2015 osa-alueista Turvallisuusjohtamisen (T) osa-alueesta Henkilöstöturvallisuus osio ja kokonaisuudessaan sekä Fyysisen turvallisuus (F) että Tekninen tietoturvallisuus. Työn ulkopuolelle rajattiin myös kaikki muut turvallisuuden osa-alueisiin kuuluvat tarkemmat selvitys- ja lisätyöt, kuten esimerkiksi ohjeiden teot ja prosessikuvaukset. (Katakri 2015, 4.) Ulkopuolelle jäävien osuuksien rajausta perustellaan työn laajuuden hallittavuudella sekä yksinkertaisesti siitä syystä, että yhden henkilön resurssien riittävyys ja

toteutettavan auditoinnin työmäärä haluttiin pitää suunnitelman mukaisesti kohtuullisena. Kaikkien osien mukaan ottaminen olisi tuonut myös liian suuria aikataulullisia ongelmia.

2.3 Toimintaympäristö, kohdeorganisaatio ja sidosryhmät

Opinnäytetyössä kohdeyritys nimettiin yritys X:ksi, jonka tarkoituksena oli häivyttää kohteen identiteettiä. Tästä syystä kohdeorganisaation toimintaympäristö ja auditoinnin toteutusympäristö esitetään mahdollisimman ylimalkaisesti. Kirjoitusasu on pyritty esittämään mahdollisimman anonyymisti ja yleisesti, jotta asiayhteyksillä ei paljastettaisi mitään arkaluontoista tietoa. Vaikka auditoinnin toteutusta ja toimintaympäristöä kuvataan mahdollisimman suppeasti, auditoinnista saadut kaikki analysointitulokset kuitenkin esitetään tässä opinnäytetyössä.

Toimintaympäristö, jossa auditoinnin kohdeorganisaatio toimii, on palvelukeskeinen ja toiminta tapahtuu aina asiakkaan tiloissa. Työntekijät kuuluvat ja toimivat siten aina osana, pääkonttorin henkilökuntaa lukuun ottamatta, asiakkaan turvallisuusorganisaatioon. Kohdeyritys myy asiakkailensa tarvittavia tukitoimintoja, työsuorituksia ja palveluja. Palveluyrityksen toimintasäde kattaa laajuudeltaan koko Suomen. Yrityksen kokoa voidaan kuvata henkilöstön lukumäärän nähden suureksi. EU:n standardin mukaan yritys on suuri silloin, kun se työllistää yli 250 työntekijää (EUR-lex 2003). Pääkonttorin lisäksi toimistoja löytyy monista kaupungeista ja toimintaa johtavat alueellisesti linjaorganisaatiot esimiehistöineen ja työnjohtajineen.

Tämän projektin toteutus tapahtui yhteistyössä kohdeorganisaation ylimmän johdon, linjaorganisaatiossa toimivien esimiesten ja työnjohtoon kuuluvien toimijoiden kanssa. Mainittu henkilöstö kattaa perustellusti asiantuntijuudeltaan ja toimenkvaltaan sen osajoukon, jolla on suurin vaikutus turvallisuusjohtamisessa ja sen toteuttamisessa. Hankkeen tilaajana toimi, oman toimen ohella, kohdeyrityksen johtoryhmään kuuluva turvallisuudesta vastaava henkilö.

2.4 Aiemmat tutkimukset

Turvallisuusjohtamisjärjestelmän toimivuutta on tutkinut Kirsi Levä (2003) väitöstutkimuksessaan. Turvallisuuskartoitusta suoritti Katri Sjöholm diplomityössään (2010), jossa tarkasteltiin palvelualan yrityksen turvallisuuden nykytilaa. Sjöholm arvioi työssään, miten kohdeyritys onnistui vastaamaan lain vaatimukseen turvallisuustoiminnassaan. Katakri 2015:a ei ole vielä käytettävissä vastaavanlaista turvallisuusjohtamista käsitteleviä tutkimustöitä, koska ajankohdaltaan se oli tämän työn tekemisen aikana vasta julkaistu. Katakri II -versiota on käytetty useissakin opinnäytetyöissä. (Levä 2003; Sjöholm 2010.)

Lähimpänä Katakri II:n mukaan tehtyä vastaavanlaista opinnäytetyötä edustaa Jussi Kojon (2013) opinnäytetyö vuodelta 2013. Kajo todensi Katakriin avulla viranomaisyksikön turvalli-

suusjohtamisen tason käyttäen vertailuarvona korotettua III tasoa ja rajasi esiauditoinnin käsitteeseen hallinnollisen turvallisuuden osa-alueita. Kimiläinen Mikko (2011) oli aikaisemmin toteuttanut yrityksen X henkilöstöturvallisuuden ja fyysisen turvallisuuden esiauditoinnin Kataktrin avulla. (Kojo 2013; Kimiläinen 2011.)

Auditoinnista ja Katakrista on myös löydettävissä joitakin eritasoisia tätä tutkimusaihetta sivuavia tutkimuksia aina opinnäytetöistä väitöskirjoihin asti. Aikaisempia tutkimuksia on otettu mukaan vain valikoidusti tilanteissa, joissa tuotetuilla tiedoilla löytyy kohteeseen liittyviä vertailtavia yhtymäkohtia tai jos ne ratkaisevasti tukevat tai kumoavat kohdeorganisaatiosta auditoidessa saatuja tuloksia tai havaintoja. Vertaisaineiston tarpeen mukaisella käytännöllä pyritään lisäämään käytettävän tietoperustan ja johtopäätösten laadukkuutta.

3 Tutkimuksen teoreettinen viitekehys

Tässä luvussa esitetään tutkimuksen aiheeseen liittyvää pohdintaa tieteenfilosofiselta kannalta ja perustellaan tutkimuksen lähtökohdista valittuja tutkimusongelmia ja asetettuja kysymyksiä. Tässä luvussa käsitellään tutkimuksen teoriapohja ja perusta esittelemällä aihealueeseen liittyvät keskeiset käsitteet. Tarkoituksena on avata tutkimuksessa käytettyä ajatuksenkulkua ja logiikkaa, jotta tutkimuksen mukainen tavoite ”kehittämiskohteiden löytäminen” tulisi paremmin ymmärretyksi ja tuloksista tehdyt johtopäätökset paremmin perustelluiksi.

Tämän tutkimuksen perimmäinen tavoite on ollut löytää hallinnollisen turvallisuuden kehittämiskohteita ja tutkimuksessa on pidetty aiheellisena myös selvittää itse tavoitteeseen sekä tulokseen vaikuttavia että merkitseviä syy-seuraussuhteita. Kausaalisten syiden selvitysosuutta on pidetty tärkeänä, jotta analyysien ja tulosten tulkinnat eivät jäisi pelkkien toteamusten ja havaintojen varaan. Tutkimuksessa ei tyydytä siten vain puutelistan esittämiseen vaan laajempaan organisaation turvallisuuskulttuurin ymmärtämiseen, jotta nykytilannetta voidaan selittää paremmin ja kehittämisehdotuksia esittää kokonaisvaltaisemmin. Tutkimuksen metodista halutaan erityisesti tuoda esiin ajatusta, että on hedelmällisempää löytää ilmiöistä ja kehityskuluista selittäviä ja korjattavia kohteita kuin yksioikoisesti tulkita ja tarkastella vain saatuja tuloksia ja tehdä niistä johtopäätöksiä.

3.1 Teoreettinen pohdiskelu, tutkimusongelma ja -kysymykset

Ensin tutkimus on asemoitava tieteellisten toimintatapamallien mukaisesti. Hirsjärven, Remksen ja Sajavaaran (2009) mukaan tutkimuksessa on selvitettävä tieteenfilosofisia kysymyksiä, sillä niihin liittyy paljon piileviä perusolettamuksia. Tämä vaatimus koskee kaikkea tutkimusta, riippumatta siitä mikä filosofinen viitekehys on ja vaikka se olisikin hyvin käytännöllistä tai työelämän sovelluksiin tähtäävää empiiristä työtä. Filosofisten lähtökohtien ym-

märtämistä pidetään tärkeänä, koska tutkimuksellisia ratkaisuja on helpompi ymmärtää, kun niille löytyy järkeenkäypiä perusteluja. (Hirsjärvi ym. 2009, 125 - 126.)

Tieteenfilosofiselta lähtökohdaltaan tämä tutkimus lähtee systeemiteorian vaikutuksesta ja oivalluksesta, että ihmisten ja työyhteisöjen toiminnan tutkiminen on vaikeaa, koska ne eivät monisäikeisyydessään ole ”yksiselitteisiä”, ”täsmällisiä” eikä edes ”kausaalisia”. Tässä tutkimuksessa painotetaan edellä mainitusta syystä hermeneuttista tutkimusotetta ja analyysimenetelmää, joka tarkoittaa, että mielenkiinto kohdistetaan ihmisten ja työyhteisöjen toiminnan ymmärtämiseen ja tulkintaan. Hermeneuttista tapaa toiminnan ymmärtämisessä ja analysoinnissa toteutetaan kuvattaessa kohdeorganisaation hallinnollisen turvallisuuden nykytilaa ja tasoa. Kohdeorganisaation toiminnan erityispiirteet pyritään ottamaan huomioon, kun saatuja arviointituloksia ja niistä tehtyjä tulkintoja tehdään. Lopputuloksena laadittu kehitysehdotus on myös tästä syystä pyritty rakentamaan yrityksen toimintoja vastaavaksi ja vastuujalon mukaisesti. Systeemiteorian filosofiset vaikutukset heijastuvat tämän tutkimuksen teoreettisten lähtökohtien taustalla, jossa korostuu pyrkimys ymmärtää paremmin ja käsitellä tapahtumaketjujen kausaalisuutta, onnettomuuksien syntymistä, inhimillisiä tekijöitä ja hallinnollisen turvallisuuden toimivuutta kokonaisuutena.

Tätä tutkimusta ohjaa ajatus, että kaikki yrityksessä toteutuneet uhat, vaarat, vahingot ja häiriöt johtuvat yrityksen turvallisuusjohtamisjärjestelmässä ilmenevistä puutteista. Ajatus kumpuaa Kerkon (2001, 14) esittämästä tutkimustuloksesta, jonka mukaan yrityksessä tapahtuvat toimintahäiriöt, vahingot ja onnettomuudet johtuvat 90 prosenttisesti inhimillisistä tekijöistä ja johtamisjärjestelmässä esiintyvistä puutteista. Myös Levä (2003, 13) väitöskirjassaan lähtee samoista tutkimuksellisista lähtökohdista ja ajatuksista liikkeelle tutkiessaan turvallisuusjohtamisjärjestelmien toimivuutta suuronnettomuusvaarallisissa laitoksissa.

Tässä tutkimuksessa tutkimusstrategiaksi, joka Hirsjärven (ym. 2009) mukaan terminä tarkoittaa tutkimuksen menetelmällisten ratkaisujen kokonaisuutta, on valittu tapaustutkimus (case study). Tapaustutkimuksen tyypillisimmät piirteet ilmenevät yhtenevinä tämän tutkimuksen kanssa siinä, että on valittu joukko tapauksia yhdestä työyhteisöstä, jossa kiinnostuksen kohteena ovat hallinnollisen turvallisuusjohtamisen prosessit ja joiden yhteyttä luonnolliseen ympäristöönsä sekä tilanteita tutkitaan keräämällä aineistoa useita menetelmiä käyttämällä. Tapaustutkimuksen tavoitteena on kuvailla toimivuutta ja tyypillisimpiä ilmiöitä mm. dokumentteja tutkien, haastatteluin ja havainnoin. (Hirsjärvi ym. 2009, 128 - 131.)

Tämän tutkimuksen pääasiallisena lähestymistapana käytettiin laadullista eli kvalitatiivista menetelmää. Haastatteluilla tuotettiin laadullista tutkimusaineistoa sekä samalla tutkittiin dokumentteja ja tehtiin havaintoja. Tutkimuksessa käytettiin hyväksi myös strukturoiduista kyselyistä saatua kvantitatiivista tietoa. Määrällistä tutkimusaineistoa tuotettiin, Likertin as-

teikon mukaisiksi, numeromuotoisiksi laadituilla kyselyillä. Molempien suuntausten käyttö nähdään enemmän toisiaan täydentävänä kuin kilpailevana lähestymistapana. (Reiman ym. 2008, 431.) Likertin asteikon mukaan laaditussa kyselyssä on esimerkiksi sekä kielteisiä että myönteisiä asenneväittämiä. Vastaaaja valitsee yhden vaihtoehdon eli mielipiteensä vaihtoehtoon, joissa yleensä käytetään 3 - 7 -portaista vastausasteikkoa (Taanila, A. 2014, 26).

Tutkimuksella on aina tehtävä ja tarkoitus, jotka ohjaavat tutkimusstrategisia valintoja ja päätöksentekoa. On pohdittava, mitä tutkitaan, mitä aineistoa kerätään ja millä menetelmillä. Ongelman määrittäminen voi olla vaikeampaa, kun mietitään tutkimusongelman ratkaisemista. Tutkimuskysymysten asettelu tulee harkita tarkkaan, koska sen perusteella yleensä ryhdytään tietoaineiston keräämiseen. Tutkimuksen loogisessa suoritusjärjestyksessä on kuitenkin havaittavissa ristiriitaisuutta, koska vasta aineistoa keräämällä voi tutkimusta tehdessään tietää, mitä kysymyksiä voi tutkimukselle asettaa. Ennakkoon muotoillut tutkimuskysymykset voivat osoittautua kerätyn aineiston valossa lopulta liian triviaaleiksi, yksinkertaisen vääriksi tai mahdottomiksi tutkia. Joka tapauksessa, tieteenfilosofian ja teoreettisen ymmärtämisen lisäksi tutkimuskysymykset ovat yksi tutkimuksen perustoista, koska ne muodostavat johtajatuksen, jonka ympärille itse tutkimustyö rakentuu. (Hirsjärvi ym.2009, 119 - 126.)

Lisäselvitysten perusteella pystyttiin lopulta määrittämään tarkemmin opinnäytetyön aihe ja tutkimusongelmat. Tälle tutkimukselle asetettiin kaksi tutkimusongelmaa, jotka ovat:

- Mitä kehittämiskohteita kohdeyrityksen hallinnollisesta turvallisuudesta löytyi?
- Soveltuuko Katakri kohdeyrityksen sisäiseksi auditointivälineeksi tai jokin auditointiprosessin tai kriteeristön osa turvallisuusjohtamisen kehittämistyökaluksi?

Ensimmäisen tutkimusongelman selvittämiseksi suoritettiin auditointi, kohdeyrityksen hallinnollisesta turvallisuudesta, käyttämällä hyväksi turvallisuusauditointikriteeristöä Katakria. Katakriin auditointiprosessi toteutettiin yhden kierroksen periaatteen mukaisesti esiauditointina, jossa käytettiin hyväksi Katakri II:n ja Katakri 2015 turvallisuuskriteeristöissä esitettyjä kysymyksiä. Kohdeyrityksen nykytilan selvittämiseksi kysymysten vastauksia verrattiin elinkeinon elämänsä suositukset (EK:n) mukaiseen suositustasoon. Katakri 2015:a ei ollut eriteltävissä vastaavanlaisia tasovaatimuksia. Katakri 2015:n kriteerejä käytettiin suoraan kriteeristöissä esitettyjen perusvaatimustasojen mukaan. Kerättyjen tietojen käsittelyssä käytettiin kolmiportaista poikkeamajaottelua, joka helpotti kehittämiskohteiden analysointia ja priorisointia. Yritykseen X kohdistettu esiauditointi suoritettiin vuoden 2015 elo- ja syyskuun aikana. Nykytilan vertailussa käytettyä asteikkoa on avattu ja selvitetty tarkemmin luvun 7 alussa.

Toisen tutkimusongelman ratkaisemiseksi tutkimustyön aikana analysoitiin Katakriin soveltuvuutta ensin yleisesti turvallisuuden kehitystyövälineenä. Soveltuvuutta selvitettiin myös koko auditointiprosessin aikana käytettävyyden, hyödynnettävyyden, muokattavuuden ja arviointi-

tulosten mukaan. Toista tutkimusongelmaa pyrittiin myös tarkastelemaan kohdeorganisaation näkökulmasta, jossa Katakrista etsittiin ja koottiin hyödyllisiä ominaisuuksia. Kohdeorganisaation jatkokehitystarpeita suunniteltaessa ajatuksena oli selvittää, miten hyvin auditointia voitaisiin tulevaisuudessa jatkaa samalla työvälineellä, nyt ulkopuolelle rajattuihin osa-alueisiin.

3.2 Keskeiset määritelmät ja käsitteet

Työn kannalta keskeisimmät käsitteet ja tietoperusteet koostuvat riskienhallinnasta, turvallisuusjohtamisesta, turvallisuusjohtamisjärjestelmästä, auditoinnista ja kansallisen turvallisuusauditointikriteeristö Katakrista. Opinnäytetyön tietoperusta rakentuu esitettyjen käsitteistöjen ympärille rakennetusta viitekehyksestä, esitetyistä teoriomalleista ja käytettävistä teorialähteistä, joiden lisäksi esitellään lyhyesti myös turvallisuusjohtamisjärjestelmiä.

Laadukkaita turvallisuusjohtamisjärjestelmiä on useita, mutta tässä työssä esitellään vain pintapuolisesti yhtä OHSAS 18001 järjestelmästandardia. Turvallisuusjohtamisjärjestelmiä ovat standardit ISO 9001 laadunhallinta, ISO 14001 ympäristöjohtaminen ja OHSAS 18001 työterveys- ja työturvallisuusjohtaminen. Turvallisuusjohtamisjärjestelmä käsitettä on selitetty tarkemmin tämän luvun alaluvussa 3.6. Turvallisuusauditointikriteeristö Katakri, joka ei ole johtamisjärjestelmä vaan auditointityökalu, on käsitelty erikseen omassa luvussa 4.

3.3 Onnettomuuksien syntyminen ja inhimilliset tekijät

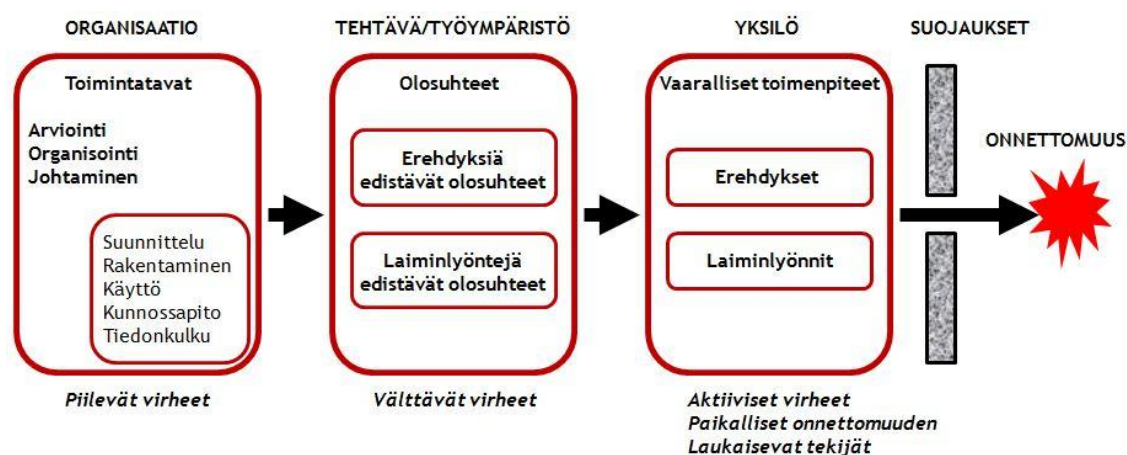
Tässä alaluvussa käsitellään aluksi onnettomuuksien syntymiseen ja inhimillisiin tekijöihin liittyviä teorioita ja kehitettyjä malleja. Samalla esitetään, miten onnettomuuksia ja vaaratilanteita syntyy, koska kriittisesti ja analyyttisesti arvioiden vältettävien tapahtumien kehityskulkuun, itse kehittämisen kohteeseen, voidaan parhaiten vaikuttaa niiden syntysijoilla. Tarkoitus on näiden teorioiden kautta ymmärtää paremmin syy-seuraussuhteita ja merkitystä sille, mitä asioita tulee organisaation johtamistoimintaan ja turvallisuusjohtamiseen sekä hallinnolliseen turvallisuuteen liittyvissä kehittämissasioissa kiinnittää erityisesti huomiota.

Samaa kausaalista paradigmaa käytetään perustellessa inhimillisten tekijöiden osuuden vaikutusten tutkimista ihmisten turvallisuuskäyttäytymisessä ja käsiteltäessä sitä tässä osioissa. Lähtöoletuksena oli ajatus, että jos mahdollisen ongelman tai vaaran eliminointi onnistuu ennen kuin se edes syntyy, olisi silloin yksi yritysturvallisuuden perustavoitteista jo saavutettu. Kerkon (2001, 38) mukaan ennaltaehkäisevä toiminta on avainsana nykyiselle turvallisuustoiminnalle ja tämän johtopäätöksen mukaan yrityksessä on siis aina käytettävä myös ne kaikki pienetkin toteuttamiskelpoiset keinot, joilla voidaan lisätä yrityksen kokonaisturvallisuutta.

Tapaturmat ja onnettomuudet katsottiin ennen aiheutuvan fyysisistä vaaroista tai olosuhteista. Turvallisuutta pyrittiin parantamaan ja onnettomuuksia vähentämään suojaamalla tuotannossa käytettäviä koneita sekä lisäämällä tuotantotilojen siisteyttä ja järjestystä. Ensimmäisen, turvallisuuden kehittämisen kannalta, käännteentekevän teorian esitti Heinrich vuonna 1931. Heinrichin esittämä ja nyt yleisesti tunnettu ”domino-teoria” perustui oletukseen, jossa onnettomuuden synty voidaan kuvata perättäisten tapahtumien ketjuna. Hänen mukaansa oleellisinta onnettomuuksien ehkäisemisessä oli eliminoida työntekijöiden vaaralliset toimenpiteet tai työympäristön vaarat fyysisissä tai sosiaalisissa olosuhteissa. (Levä 2003, 19.)

Monet tutkijat ovat myöhemmin kehittäneet Heinrichin teoriaa eteenpäin. Levän mukaan Bird & Loftus (1976) laajensivat Heinrichin mallia, joka huomio myös johtamisen vaikutukset onnettomuuksien syntymiseen ja niistä seuranneisiin vaikutuksiin. Myöhemmin Bird & Germain (1986) määrittivät pääasialliseksi, onnettomuuksien synnyn ja vakavien seurausten, syyksi puutteet yritysjohdon valvonnassa. Kuusiston mukaan Petersen (1988) laajensi myös osaltaan teoriaa yksittäisistä toimista ja olosuhteista aina johtamisjärjestelmään saakka. Petersen päätteli tällöin, että vaaralliset toimenpiteet, vaaratekijät ja onnettomuudet ovat kaikki oikeita organisaation johtamisjärjestelmän puutteista. Petersen korosti ylimmän johdon vastuuta sellaisen järjestelmän luomisessa, jolla tehokkaasti voidaan hallita yrityksen toimintaa uhkaavat vaarat. (Levä 2003, 19; Kuusisto 2000, 26.)

Organisaatioissa, ylempien toimihenkilöiden, päätökset ja toimet vaikuttavat välittömästi työntekijöiden työolosuhteisiin, toimintaan, käyttäytymiseen ja riskinottoon. Kaikki toimintaedellytyksien puutteet ja heikkoudet organisaation toiminnassa edesauttavat piilevien syiden ja välittömien virheiden syntymisessä sekä niistä johtuvien suojausten pettämisessä. (Levä 2003, 20.)



Kuvio 1: Aktiiviset ja piilevät virheet onnettomuuksien syntymisessä (Levä 2003, 19)

Reason toi onnettomuuksien syntymalliin uusina käsitteinä sekä aktiivisen että piilevän virheen (kuvio 1). Reasonin mukaan aktiiviset virheet ovat niitä, joita työntekijä tekee joko erehdyksestä tai laiminlyönnistä. Yhdessä työntekijän aktiivisen virheen kanssa suojauksen rikkoutuminen johtaa yleensä nopeasti onnettomuuden syntymiseen. Piilevät virheet kumpuavat johdon tekemistä päätöksistä tai toimenpiteistä, jotka jäävät usein ”kytemään”. Piilevät virheet ilmenevät tai laukeavat yhdessä ja samanaikaisesti aktiivisten virheiden kanssa esimerkiksi työntekijän toimenpiteen sekä teknisen vikaantumisen yhteisvaikutuksesta. Piilevät virheet saavat alkunsa päätöksen tekijöistä, suunnittelusta ja organisaation toiminnasta. Reason korostaa myös, että vaikka onnettomuuksia ei olisi vielä tapahtunut, organisointi- ja menettelytapavirheet ovat silti voineet jäädä piileviksi virheiksi organisaation toimintoihin. (Levä 2003, 19; Reason 1997.)

Myöhemmin Reason kehitti yleisemmin tunnetun ”reikäjuustomallin”. Reasonin onnettomuuksien ja vaaratilanteiden syntymalli perustuu ajatukseen, jossa monimutkainen järjestelmä suojataan monipuolisilla ja moninkertaisilla haittatapahtumien estoilla. Suojaukset voivat olla ihmisten toimia, organisatorisia menettelyitä tai teknisiä ratkaisuja. Suojausten tarkoituksena on toimia suojaavina mekanismeina ja turvallisen menettelyn varmistajana, jotka toimivat ihannemaailmassa virheettöinä ja täydellisesti. Jos suojaukset perä jälkeen pettävät tai niitä ei ole riittävästi, onnettomuus tai vaara pääsee tapahtumaan. Mallissa suojaus kuvataan reikäjuustona, jossa on suojauksien lukumäärän mukaan asetettu perä jälkeen reikäjuustoviipaleita ja itse reiät merkitsevät suojauksien pettämistä. Juustoon kuvatut reiät voivat syntyä välittömässä toiminnassa tapahtuneina virheinä tai ajallisesti etäällä ja organisaatiossa ylempänä tehdyistä ratkaisuista ja päätöksistä johtuen. Kun kaikkien onnettomien sattumien summana nuo reiät asettuvat suoraan linjaan, toiminnallinen tapahtuma etenee kaikkien suojausten läpi synnyttäen onnettomuuden tai aktivoiden vaaratilanteen. (Levä 2003, 19; Reason 1997.)

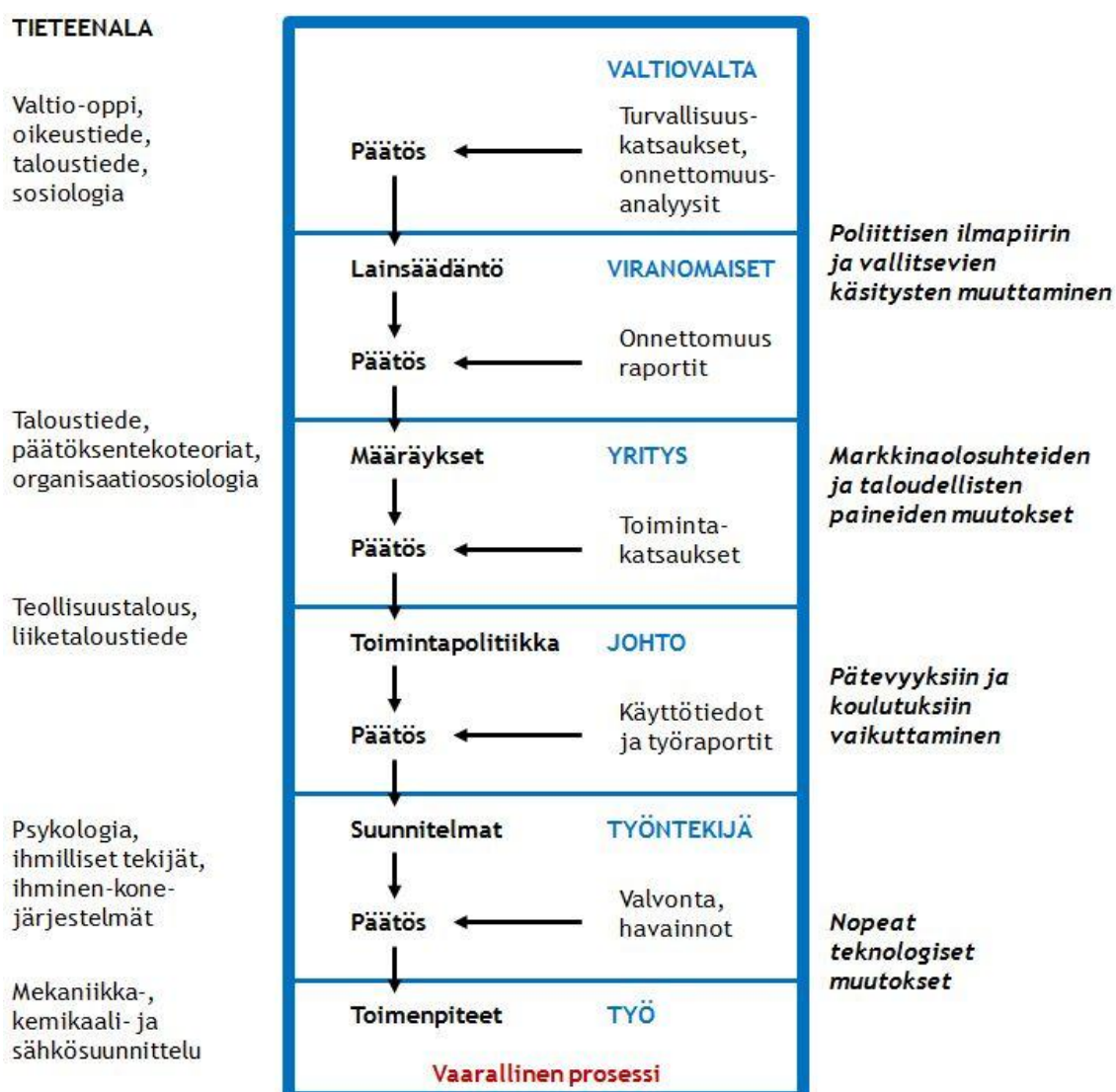
Edellä esitettiin teorioita siitä, että onnettomuuksiin johtavat syyt, johtuvat organisaation toiminnassa piilevistä syistä ja yrityksen johdon tekemistä virheellisistä päätöksistä. Muut syyt, jotka vaikuttavat myös työntekijän käyttäytymiseen, toimintaan ja päätöksiin, kuten inhimilliset virheet, ovat jääneet vielä täysin huomioimatta. Inhimilliset virheet tapahtuvat eri syistä kuin edellä on kuvattu ja niiden ehkäisy vaatii myös erilaisia toimenpiteitä.

Levän mukaan Kletz (1991) jakaa inhimilliset virheet ja niitä ehkäisevät toimenpiteet seuraavasti:

1. *Lipsahdukset tai tilapäiset huomiovirheet*, joiden tarkoitus on oikea, mutta teot tai toimenpiteet ovat vääriä tai ne jätetään kokonaan tekemättä - Virheen toteutumismahdollisuuksia voi vähentää työolosuhteita muuttamalla.
2. *Puutteellinen koulutus tai virheet ohjeissa*, johtaa tilanteisiin, joissa henkilö ei tiedä mitä pitäisi tehdä tai vielä pahempaa on, että käytettävissä olevat tiedot ovat vir-

heellisiä ja tehdään väärää toimenpiteitä - Virheen toteutumismahdollisuuksia pienennetään parantamalla koulutusta tai ohjeita tai työtä yksinkertaistamalla

3. *Henkilön fyysiset tai psyykkiset kyvyt eivät vastaa tehtävään vaadittua suoritusvaatimusta.* Virhemahdollisuuksia pienennetään muuttamalla työolosuhteita.
4. *Harkittu päätös toimia päinvastoin kuin on sovittu ohjeiden noudattamisesta tai hyväksytystä toimintatavasta toimia.* Voi johtua laiminlyönnistä tai oletuksesta, että ohje on väärä. Tahallisen sääntöjen rikkomisen ja tarkoituksellisen toiminnan välillä on suuri ja selvä ero. Selvitettävä, virhemahdollisuuksien vähentämiseksi, miksi ei noudateta ohjeita. (Levä 2003, 20 - 21.)



Kuvio 2: Rasmussenin sosio-tekninen onnettomuusketjun järjestelmämalli (Levä 2003, 22)

Reason (1990) puolestaan jakaa inhimilliset virheet kolmeen virheluokkaan, jonka jaottelun alkuperä perustuu Rasmussenin (1986) kolmen luokan mukaiseen ihmisen toiminnan malliin:

1. *Taitopohjaiset virheet* voidaan jakaa hajamielisyteen ja lipsahduksiin, joissa itse toiminta tutun tehtävän parissa on hyvin opeteltua, rutiininomaista ja automaattista. Esimerkkinä tällaisesta toiminnasta on vaihteen vaihtaminen epähuomiossa väärin.
2. *Sääntöpohjaiset virheet* ovat niitä, joissa noudatamme ja sovellamme kirjallisia ohjeita, kuten hyvien sääntöjen väärinkäytössä sekä väärän säännön käyttämisessä. Esimerkkinä tästä on yleissääntöjen noudattaminen, kuten odottaminen rauhassa kolme päivää lapsen kuumeilua, ennen kuin on sallittua harkita lääkäriin menoa.
3. *Tietopohjaiset virheet* ovat tietoista ongelmanratkaisua uudenlaisen ongelman kohdalla, joihin ei ole olemassa vielä sääntöjä. Virhe syntyy päättelyn harhoista, kun tehtävää ollaan suorittamassa ensimmäistä kertaa. Kun toimija ei tiedä, jonkin ilmiön mahdollisuudesta, ei siihen osaa myöskään oikein varautua. (Reiman ym.2008, 196.)

Tieteen eri alat ovat tutkineet rajoitetusti omasta näkökulmasta onnettomuuksien syntyä. Rasmussen (1997) on näiden tutkimusten kautta pohtinut esitettyjen mallien riittävyyttä nykyisessä dynaamisessa maailmassa ja esittänyt oman sosio-tekniikan riskienhallintamallinsa. Rasmussenin (1997) malli muodostuu monista tasoista: lainsäätäjät, yrityksen ylin johto, suunnittelijat ja henkilöstö. Malli painottaa nopeiden muutosten huomioonottamista, joita ovat: teknologiset, kilpailuympäristölliset, säädösten ja julkisten paineiden vaikutukset yrityksen toimintakentässä. Rasmussen (1997) lähtee siitä, että dynaamisessa sosio-tekniikassa yhteiskunnassa ilmenee eri tasoilla riskitekijöitä, jotka edesauttavat onnettomuuksien syntymistä (kuviokuva 2). Rasmussenin (1997) malli luo sen kokonaiskuvan tekijöistä, jotka vaikuttavat ihmisten ja organisaatioiden toimintaan. (Levä 2003, 21; Rasmussen 1997, 183 - 213.)

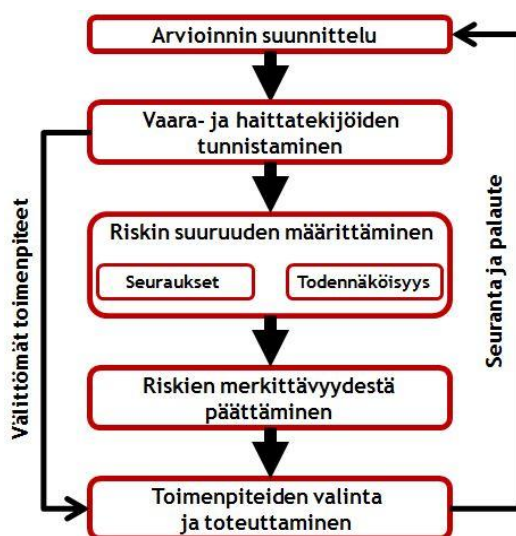
Onnettomuuksien ehkäisyvaatimusten taustalla oleva käsitys korostaa tarvetta kehittää turvallisuusjohtamista, turvallisuuslainsäädäntöä ja viranomaisvalvontaa. Rasmussenin (1997) malli ottaa nyt huomioon yrityksen ulkopuolisten tekijöiden vaikutukset vaara- ja onnettomuustekijöiden syntymisessä. Tämä johtaa väistämättä päätelmään, että riskien hallinta, onnettomuuksien syntymisen ehkäiseminen ja turvallisuuden parantaminen edellyttää, että järjestelmän eri tasoissa olevia vaaratekijöitä arvioidaan mahdollisina onnettomuuksiin johtavina tapahtumaketjuina. (Levä 2003, 21; Rasmussen 1997, 183 - 213.)

Yhteenvetona voidaan todeta, että turvallisuusjohtamisen menetelmiin vaikuttaa kaikkein eniten ja suoraan, tiedostamatta tai tietoisesti, lineaariset onnettomuusmallit. Riskikäyttäytymiseen pohjautuva turvallisuusohjelmat näkevät vaarallisten tekojen karsimisen vaikuttavan eniten onnettomuuksien syntymisen vähenemiseen. Johtopäätös on myös, että esimiesten parhaimmat keinot ja suurimmat vaikuttamismahdollisuudet vähentää onnettomuuksia ja väärää inhimillistä käyttäytymistä ovat ohjeistus, koulutus ja työntekijöiden toiminnan valvonta.

Lineaariset mallit eivät kuitenkaan ota huomioon mm. ympäristötekijöiden vaikutusta, eivätkä erilaisia suojauksia tai edes piileviä virhetiloja, kuten esimerkiksi huonoa koulutusta. Kaikki edellä mainitut vaikuttavat omilta osiltaan virheiden, vaarojen ja onnettomuuksien syntymiseen. Onnettomuusmallit eivät ota myöskään huomioon tapahtumakentän monimuotoisuutta eivätkä sitä, että onnettomuuksien syntymiseen vaikuttaa monia kausaalisia tekijöitä, jotka eivät pelkästään johdu inhimillisistä tekijöistä tai turvallisuusjohtamiseen liittyvistä puutteista. (Reiman ym.2008, 197.)

3.4 Riskienhallinta

Työturvallisuuslain (738/2002) 10 §:n 1 momentin mukaan edellytetään, että työnantaja järjestelmällisesti selvittää ja tunnistaa työstä, työtilasta, työympäristöstä ja työolosuhteista aiheutuvat haitta- ja vaaratekijät sekä arvioi niiden merkityksen työntekijöiden turvallisuudelle ja terveydelle. Tämä tarkoittaa, että työnantajan on aina ja kaikkialla toimintaympäristöstä selvitettävä ja kartoitettava kaikki riski- ja uhkatekijät, joita sen työntekijä voi eri tilanteissa ja olosuhteissa kohdata ja arvioitava asetettujen suojaustoimien riittävyys. Kuten lain nimestäkin voi jo päätellä, se ei kuitenkaan ota huomioon yrityksen kaikkia riskejä.

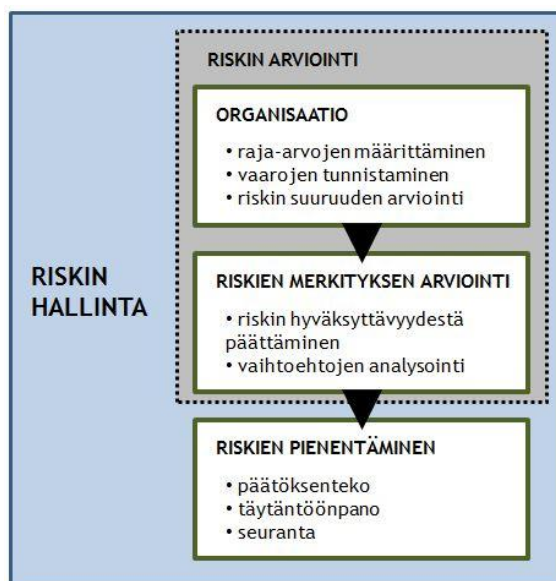


Kuvio 3: Riskienarvioinnin vaiheet, yksinkertaistettu kehämalli (Riskin arviointi 2013, 10)

Turvallisuusjohtamisen perusta luodaan riskienhallinnalla. Riskienhallinta alkaa riskien tunnistamisesta ja jatkuu riskien toteutumisen todennäköisyyksien arvioimisella. Riskienhallinnassa noudatetaan jatkuvan uudelleenarvioinnin kehämallia (kuvio 3), jotta toimintaympäristön muutokset tulevat huomioitua. Riskienhallinta on systemaattista toimintaa, jonka tarkoitus on varmistaa toiminnan häiriöttömyys. Riskeihin voidaan varautua niitä estämällä, vähentämällä,

siirtämällä, vakuuttamalla tai jatkuvuussuunnitelmilla. Riskienhallinta on osa jokapäiväistä toimintaa, jolle on määritelty tarkoitus, tavoitteet, roolit ja vastuut. Yrityksen riskit kohdistuvat sen henkilöstöön, omaisuuteen, tietoon, ympäristöön ja maineeseen, kuten elinkeinon keskusliiton turvallisuusjohtamisen ympyrässä on kuvattu yrityksen arvoja, joita turvallisuustoiminnalla suojataan (kuvi 5). Yrityksen pyrkimys on riskienhallintamallin käytönotolla varmistaa toimintojensa tarkoituksenmukaisuus ja tehokkuus, tiedon ja raportoinnin luotettavuus sekä sääntelyn noudattaminen. (Paasonen ym. 2012, 80 - 85.)

Riskienhallinta määritellään yrityksen kokonaisvaltaiseksi toiminnaksi vaarojen ja uhkien tunnistamiseksi ja niiden aiheuttamien haittojen ja vahinkojen estämiseksi, minimoimiseksi ja valvomiseksi (Reiman ym. 2008, 433). Työsuojeluhallinto määrittelee riskienhallinnan systemaattiseksi toiminnaksi riskien tunnistamisessa, arvioimisessa ja pienentämisessä. Riskienhallinnan osa-alueet ovat: riskien arvioinnin osassa sekä riskianalyysi että riskien merkityksen arviointi ja lopuksi päätökset riskien pienentämiseksi (kuvi 4). (Työsuojeluhallinto 2014.)



Kuvio 4: Riskienhallinnan osa-alueet (Riskin arviointi 2013, 6)

Riskienhallinnan standardin ISO 31000 avulla yritykset voivat kehittää riskienhallintaansa ajan ja vaatimusten mukaiselle tasolle. Standardin avulla voidaan luotettavalla tavalla tunnistaa, hallita ja ottaa tietoisia riskejä. Standardin käytön kautta yritys lisää todennäköisyyttä saavuttaa tavoitteensa kykenemällä tunnistaa riskientunnistamistarpeensa ja käsitellä riskejä. Standardi edesauttaa myös kehittämään hyvää hallintotapaa, ennakoivaa johtamista ja raportointia. Standardista ei ole sertifiointin perustaksi. (ISO 31000 2013.)

Riskienhallinnassa lähdetään siitä, että tunnistamattomia riskejä ei voi hallita, koska niihin ei voi ennakoivasti varautua. Riskienhallinnalla pyritään erilaisia analysointimenetelmiä monipuolisesti hyödyntämällä havaitsemaan ja tunnistamaan ennakolta riski- ja vaaratilanteita. Tunnistusmenetelmien perusteella on pystyttävä arvioimaan riskin mahdollisuus, todennäköisyys ja niistä johtuvat seuraukset. Tunnistuksella voidaan saada näkyviin myös piilossa olevia riskejä, mitkä eivät muuten olisi havaittavissa. (Flink, Reiman & Hiltunen 2007, 131, 136.)

Riskejä hallitaan järjestelmällisellä riskien arvioinnilla. Riskien arviointiin kuuluu riskien tunnistaminen, tunnistettujen vaarojen ja uhkien riskianalyysi sekä merkityksen arviointi. Riskejä tulee arvioida niiden suuruuden mukaan, jotka määräytyvät esiintymisen todennäköisyyden ja seurausten perusteella. Riskien tunnistamisessa ja arvioimisessa on tärkeää suorittaa kokonaisvaltainen sekä kattava kartoitus välttämällä tekemästä yksittäisiä tai toisistaan irrallisia arviointeja, tarkasteluja tai selvityksiä. Riskien käsittelyssä tehdään päätöksiä jatkotoimista ja hyväksyttävästä riskitasosta sekä mitä riskejä ollaan valmiita sietämään. (Levä 2003, 53.)

Riskiperusteinen turvallisuusjohtaminen kattaa kaikki turvallisuuden osa-alueet, missä järjestelmällinen ja kokonaisvaltainen riskienhallinta toimii turvallisuusjohtamisen työvälineenä. Riskienhallinnan osaaminen tai riskienhallintamallin puuttuminen organisaatiossa muuttaa olennaisesti koko turvallisuusjohtamisen luonnetta. Tunnistamattomiin riskeihin ei pystytä varautumaan eli turvallisuutta ei hallita ennakoivasti, jolloin ennakoimaton toteutunut riski saattaa lamauttaa pahimmassa tapauksessa koko toiminnan. Sama vaara on tunnistettujen riskien kohdalla, jos niitä ei arvioida tai käsitellä oikein. Riskien tunnistamista ei kannata jättää pelkästään tapahtuneiden onnettomuuksien tai läheltä piti vaaratilanteiden varaan. On myös huomioitava, ettei riskitöntä organisaatiota ole olemassakaan ja kaikkiin riskeihin ei ole toimivaa tai järkevää hallintakeinoa käytettävissä, mutta niitä voidaan vaimentaa tai siirtää.

3.5 Turvallisuusjohtaminen

Yksinkertaisuudessaan turvallisuusjohtaminen on vuosikellon mukaista säännöllistä toimintaa, johon Kerkon (2001, 12) mukaan kuuluvat seuraavat riskienhallintatoiminnan etenemisvaiheet:

1. Kartoita ja tunnista vaarat
2. Arvioi ja päätä toimenpiteiden tarpeellisuus
3. Suunnittele tarvittavat toimenpiteet
4. Toteuta toimenpiteet

Turvallisuusjohtaminen on Lanteen (2007, 12) mukaan järjestelmällistä ihmisten, omaisuuden, tiedon, maineen ja ympäristön suojelemiseen tähtäävää ennaltaehkäisevää ja päämäärätietoista sekä jatkuvaa turvallisuuden prosessimaista kehittämistoimintaa. Organisaation tur-

vallisuusjohtamisen tulostavoitteena on suojata ennakolta vaaratilanteilta, vahingoilta, onnettomuuksilta ja rikolliselta toiminnalta. Turvallisuusjohtamisella taataan yrityksen toimintaedellytykset ja toiminnan häiriöttömyys sekä luodaan valmiudet jatkaa toimintaa normaalioloissa tapahtuvista häiriöistä huolimatta. (Kerko 2001, 21.)

Levän (2003, 35 - 36.) mukaan turvallisuusjohtamistoiminnan onnistumiseen liitetään seuraavia piirteitä:

- Yrityksessä on asetettu turvallisuustavoitteet, joita seurataan
- Yrityksessä on laadittu kirjallinen turvallisuuspolitiikka
- Turvallisuusvastuut on määritelty kirjallisesti korostamalla linjaorganisaation vastuita
- Johto on henkilökohtaisesti sitoutunut turvallisuuteen ja osoittanut sen käytännössä
- Johto on perehdytetty ja koulutettu turvallisuusjohtamiseen
- Esimiehet valvovat turvallisuutta ja puuttuvat riskinottoon nopeasti
- Henkilöstö on turvallisuusasioihin perehdytetty ja koulutettu sekä informoitu
- Henkilöstön turvallisuuskoulustarpeet on huolellisesti kartoitettu
- Henkilöstö on tehokkaasti motivoitu, osallistutettu ja valtuutettu turvallisuustyöhön
- Turvallisuusasiantuntijat ovat päteviä ja antavat riittävästi tukea
- Riskit tunnustetaan sekä niiden seurausten vakavuutta arvioidaan säännöllisesti
- Laitteistojen huolto- ja kunnossapitotoimia toteutetaan ennakoivasti
- Prosessien ja ohjeistuksen käytön suunnittelussa huomioidaan aina myös turvallisuus
- Vaaratilanteet ja onnettomuudet tutkitaan ja niistä opitaan
- Häätätilanteita ja poikkeustilanteita varten laaditaan varautumissuunnitelmia
- Sisäisiä auditointeja toteutetaan
- Turvallisuustoimintaa mitataan proaktiivisesti
- Yleistä siisteyttä ja järjestystä ylläpidetään
- Turvallisuusohjelmia laaditaan ennaltaehkäisevästi
- Turvallisuuskulttuuria kehitetään jatkuvasti

Turvallisuusjohtamista ei pidä käsittää pelkästään lainsäädännöllisten velvoitteiden ja rikosoikeudellisten vastuiden täyttämisen työvälineenä. Organisaatiot kohdistavat turvallisuusjohtamisessa suurimman huomionsa henkilöstöturvallisuuteen. Henkilöstöriskejä vähennetään työturvallisuuslakia noudattamalla ja se on tärkein turvallisuusajattelun osa-alue. Kerkon (2001) mukaan normikeskeisyys kattaa ainoastaan noin 10 prosenttia organisaation kokonaisturvallisuuden kentästä. Vaikka lainsäädäntö on kehittynyt työolosuhteiden, työvälineitten ja terveydenhuollon sekä fyysisten rakennus- ja paloturvallisuusmääräysten mukaan, turvallisuusjohtamista on katsottava paljon laajemmasta näkökulmasta. Keskittymällä pelkästään lakien ja asetusten vaatimusten täyttämiseen organisaation kokonaisturvallisuus jää sivummalle ja turvallisuusjohtamisen kehittyminen hidastuu. (Kerko 2001, 13 - 15)

Levän (2003) mukaan kritiikkiä on kohdistettu siihen, että turvallisuusjohtamisen painopiste on ollut liiaksi hallinnollista organisointia, menettelytapojen eli asioiden johtamista (Management). Ongelmaksi on muodostunut, että turvallisuusjohtamisessa on liian vähän huomioitu ihmisten välisen vuorovaikutuksen merkitys eli ihmisten johtaminen (Leadership). Turvallisuusasioiden hallinta ei yksin riitä vaan tarvitaan enemmän inhimillistä toimintaa, jolla on vähintäänkin yhtä tärkeä merkitys turvallisuustavoitteisiin pääsemiseksi. (Levä 2003, 35 - 36.)

Kerko (2001) mainitsee määritelmässään osuvasti, että turvallisuusjohtaminen on johdonmukaista päätöksentekoa ja yhteistyötä, missä kaikki tietävät velvollisuutensa. Turvallisuusjohtamisen tulee ohjata organisaation toimintaa johdonmukaisesti ja tavoitteellisesti. Nykypäivänä on lähdettävä siitä, että ennen niin hyvin toiminut turvallisuustoiminnan tehokkuus ei enää ole vain työntekijä- ja työnjohtajatasoisen keskinäisen yhteistyön varassa ja vastuulla olevaa toimintaa. Nykyaikana turvallisuusjohtamisen on perustuttava laatu- ja liiketoimintajohtamisen malleihin, joiden mukaan ylimmän johdon toimintaan pohjautuvaa turvallisuusjohtamiskulttuuria on myös lähdettävä kehittämään. (Kerko 2001, 7, 38.)

Turvallisuusjohtamisen ja turvallisuuskulttuurin tärkeyttä arvioitaessa on huomioitava Kerkon (2001) mainitsema Pesosen (1993) väitöskirjatutkimus, jonka mukaan työntekijät ja asiakkaat suhtautuvat vastahakoisesti yritykseen, jossa turvallisuusasiat eivät ole kunnossa. Pesosen (1993) väitteen mukaan myös henkilöstön työskentely ei ole silloin tehokasta, kun energiaa sitoutuu turvallisuudesta huolehtimiseen. Pakottavasta työsuojelulainsäädännön korostuneesta osuudesta huolimatta turvallisuusasioihin ei vielääkään panosteta riittävästi, mikä kertoo nykypäivänä sen, että kun yrityksessä ei ole välttämättömiä toimia, ei yrityksessä silloin myöskin synny turvallisuusjohtamisesta johtamistraditiota. Hyvin ja tehokkaasti toteutettuna turvallisuustoiminta on kuitenkin myös muuta kuin velvoite, sillä se on myös subjektiivisen turvallisuustunteen lisäksi merkittävä liiketoimintaa kehittävä ja parantava tekijä (Kerko 2001, 15)

Koska organisaation toimintaa johtaa yrityksen johto, joka vastaa turvallisuustoiminnan organisoinnista ja käytännön työstä, on johdon toimenpiteillä sekä päätöksillä suuri vaikutus organisaation turvallisuuskulttuurin muodostumisessa. Onnistuakseen turvallisuusjohtamisessa ja johtamistavoitteissa yleensä, on organisaation ylimmän johdon myös täydellisesti sitouduttava ja noudatettava tekemiään päätöksiä uskottavan toiminnan aikaansaamiseksi. Ylimmän johdon käytännön toiminnalla ja esimerkin voimalla osoitetaan turvallisuusasioiden tärkeys ja merkitys yrityksessä. Hallinnollisesti (Management) luodut ohjeet, määräykset ja politiikat eivät yksistään riitä, ne pitää myös saattaa täytäntöön ja siinä tarvitaan henkilöstön johtamista (Leadership). Kaikille tasoille ulottuvat turvallisuutta ylläpitävät käytännöt, parantavat ja kehittävät toimet sekä panostukset luovat turvallisuuskulttuuria. (Kerko 2001, 25 - 26.)

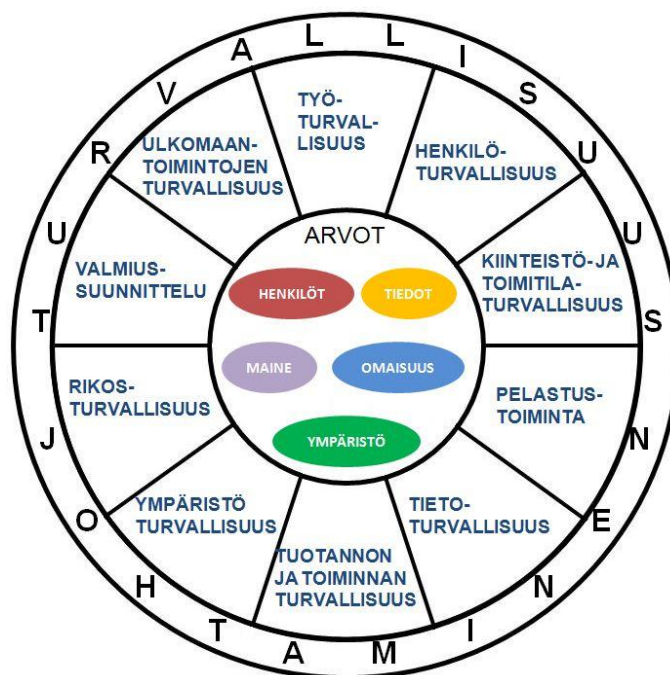
Kerkon mukaan (2001) turvallisuuskulttuurin vahvin lenkki on omilla aivoilla ajatteleva työntekijä, joka on luonnostaan mieltänyt varovaisuuden ja turvallisuuden osana ammattitaitoa. Kerko (2001) väittää, että henkilöstö, joka tekee yrityksen tuloksen, tekee myös sen turvallisuuden. Tehokkaassa turvallisuusjohtamisessa on siten kaikki oltava osallisina toimintaan liittyvissä suunnittelu- ja päätöksenteoissa, jotta päivittäisen toiminnan kehittyminen olisi taattu. Hyvä turvallisuusjohtamiskulttuuri myös kannustaa jokaisen käyttämään omaa järkeään ja luovuutta, joka myös tukee ja edistää turvallisuuden ylläpitämistä. Turvallisuusjohtamisjärjestelmän tulee myös luontevasti lisätä henkilöstön työn haasteellisuutta, palkitsevuutta ja mielekkyyttä korostamalla henkilöstön osuuden tärkeyttä. Henkilöstön sitouttaminen onnistuu parhaiten motivoimalla, kouluttamalla ja tiedottamalla. Henkilöstö tuntee samalla olevansa tärkeänä osana kokonaisturvallisuuden toteutumisessa. (Kerko 2001, 20, 23, 26.)

Levä tuo esiin Kletzin (1991) tarkastelemia turvallisuusasioiden vastuita, jonka mukaan yrityksen ylimmän johdon tulee olla aktiivinen ja säännöllisesti tunnistaa, sopia ja seurata kohteidensa turvallisuuspuutteiden korjaustoimia ja kehittää työympäristöjä turvallisempaan ja käyttäjäystävällisempään suuntaan. Samalla ylimmän johdon tulee järjestelmällisesti arvioida ja huolehtia, että työntekijöiden tietoja ja osaamista ylläpidetään riittävällä tasolla. Yrityksen johto on vastuussa myös ”lähetä piti” ja tapahtuneiden onnettomuustilanteiden perusteellisesta tutkinnasta. Johdon ei tule hyväksyä sellaisia tapahtumaraportteja, joissa käsitellään vain tapahtumiin johtaneita välittömiä syitä. On tutkittava tapahtumiin johtaneita syitä perusteellisesti, jotta organisaatio oppisi kaikista tilanteista ja muistaisi paremmin tapahtumia sekä turvallisuusosaaminen että turvallisuusjohtaminen kehittyisi. (Levä 2003, 35 - 36.)

Turvallisuusjohtamisen on perustuttava yrityksessä päätettyihin toimintaperiaatteisiin, arvo maailmaan ja strategiaan. Turvallisuusjohtamisessa noudatettavat toimintaperiaatteet tulee kirjata ylös yrityksen turvallisuuspolitiikaksi, josta pidetään myös kiinni ja siihen sitoudutaan. Turvallisuuspolitiikka on strateginen ohjelma, jonka mukaan kokonaisturvallisuutta johdetaan, ylläpidetään ja kehitetään. Turvallisuuspolitiikassa määritellään konkreettisesti ne turvallisuustoiminnassa ja johtamisessa käytettävät periaatteet, menettelytavat, laatutasot, laajuudet, tavoitteet, henkilöstön sitoutumiset, koulutuksen varmistamiset, katselmusten suorittamiset, riskien huomioimiset, vastuut, veloitteet, valtuudet ja resurssit. Turvallisuuspolitiikalla osoitetaan, että turvallisuus on tärkeä osa liiketoimintaa. (Kerko 2001, 44 - 46)

Laajaan turvallisuustoimintaan kuuluu Kerkon (2001) mukaan: turvallisuus (Safety), terveys (Health), ympäristö (Environment) ja laatu (Quality), jonka tavoitteena on integroitu SHEQ -toimintamalli. Tutkittavana ilmiönä turvallisuusjohtamisen ympärille kuuluu kaikki kymmenen yritysturvallisuuden osa-alueita, joita ovat työturvallisuus, henkilöturvallisuus, kiinteistö- ja toimitilaturvallisuus, pelastustoiminta, tietoturvallisuus, tuotannon ja toiminnan turvallisuus, ympäristöturvallisuus, rikosturvallisuus, valmiussuunnittelu sekä ulkomaantoimintojen turval-

lisuus (kuvio 5). Jotta organisaatio pystyisi hallitsemaan kaikkia edellä mainittuja turvallisuuden osa-alueita, on luotava yksi turvallisuuden yleishallintajärjestelmä, johon on integroitu mm. ympäristö- ja tietoturvasuosasioiden hallintajärjestelmät. (Kerko 2001, 20 - 21.) Katakrin mukaan hallinnollisen turvallisuuden osat ovat turvallisuusjohtamista (Katakri II 2011, 3).



Kuvio 5: Turvallisuusjohtamisen osa-alueet (Elinkeinoelämän keskusliitto)

Turvallisuusjohtamisen olennaisena osana on ymmärtää yrityksen turvallisuuskulttuuria. Johdon ja henkilöstön tulee sitoutua hyvän turvallisuuskulttuurin luomiseen, jotta organisaation turvallisuutta voidaan ylläpitää hyvällä tasolla. Turvallisuuskulttuuri kertoo organisaation kyvystä ymmärtää turvallisuutta sekä yrityksen vallitsevasta tahtotilasta, miten turvallisuusasioita ja henkilöstön motivaatiota turvallisuusasioihin hoidetaan. (Paasonen ym. 2012, 96 - 99)

3.6 Turvallisuusjohtamisjärjestelmä

Hallinnollinen turvallisuus on osa turvallisuusjohtamisjärjestelmää. Turvallisuusjohtamisjärjestelmälle on esitetty monia yleisiä määritelmiä ja kuvauksia, mutta itse järjestelmän sisältövaatimuksia on laadittu vähän ja silloinkin ne yleensä vastaavat vain tiettyä turvallisuuden osa-alueita, kuten esimerkiksi tietoturvasuosuutta. Järjestelmän sisältövaatimuksia on kohdennettu vain tiettyihin toimialoihin, kuten merenkulussa tai kansainväliseen siviili-ilmailuudessa käytettävään turvallisuusjohtamisjärjestelmään. (Kunttu 2009, 7.) Siten ei ole löydettävissä sellaista yhtä yleistettävää toimialasta tai turvallisuuden osa-alueesta riippumatonta turvallisuusjohtamisjärjestelmän sisältövaatimusta tai kuvausta. Jokaista turvallisuusjohtamisjärjes-

telmän yksityiskohtaista sisältöä ja vaatimusta tulee tarkastella erikseen turvallisuusjohtamisjärjestelmistä esitettyjen määritelmien, lainsäädännön sekä standardien avulla.

Kerkon (2001) mukaan nykypäivän turvallisuusjohtaminen on tullut tilanteeseen, jossa sille asetetaan sellaisia laajenevia toimintavaatimuksia, joita se ei enää pysty hallitsemaan ellei se integroidu organisaatioiden päivittäis-, laatu- ja liiketoimintajohtamistoimintaan. Turvallisuuslainsäädännön kehitysvauhti ja suunta sekä henkilöstöasioiden ja hyvinvoinnin hallinnointi että yritysturvallisuuden eri osa-alueiden uhkien lisääntyminen asettaa turvallisuusjohtamiselle suuret vaatimukset ja odotukset. Turvallisuusasioiden hoitaminen ei enää käy suoritettuna yrityksessä sijais- tai erillis- tai hajautustoimintoina vaan nykypäivän kokonaisturvallisuuden haasteisiin tulee vastata turvallisuusjohtamisjärjestelmän näkökulmasta. (Kerko 2001, 7 - 8.)

Turvallisuusjohtamisjärjestelmä on nykypäivänä liiketoiminnan vaatimusten kannalta tärkeä, sillä ilman sitä organisaation on vaikea toimia. Turvallisuusmääräysten noudattaminen ja lainsäädännön muutoksissa mukana pysyminen edellyttää turvallisuusjohtamisjärjestelmälle ominaisia suunnittelu-, hallinta- ja muutosprosessien käyttöä. Organisaation toimintaympäristössä tapahtuvat nopeat kilpailu-, sopimus- ja joustavuusvaatimuksien tai velvoitteiden muutokset asettavat muutoksenhallintakyvylle huomattavia lisähaasteita. Nopeatempoisessa ja dynaamisissa tilanteissa ilmenneet kokonaisturvallisuuden järjestelmäpuutteet voivat haitata liiketoimintaa, rekrytointia tai estää jopa yhteistyösopimusten syntymisen. (Kerko 2001, 32.)

Yhden johtamisjärjestelmän tarkoitus on tuottaa suurempaa synergiaetua kuin useat erilliset järjestelmät, joita käytetään yhtäaikaisesti. Turvallisuusjohtamisjärjestelmällä on paljon yhteistä laatujohtamisjärjestelmän kanssa, jossa ei kuitenkaan vielä ole vakiintunutta sisältöä ja mallia. Ongelmaksi on muodostunut se, että järjestelmä huomioi vain jonkin tietyn valitun turvallisuuden osa-alueen. Laatujohtamisen ja turvallisuusjohtamisen merkittävin yhtäläisyys on kuitenkin kokonaisuuden johtaminen ja hallinta, joissa molemmissa korostuvat seuranta, mittaaminen, henkilöstön sitouttaminen ja dokumentointi. (Paasonen ym. 2012, 93 - 96).

Levän (2003) mukaan turvallisuusjohtamisjärjestelmä on kokonaisuus, joka voidaan mallintaa yhdeksi järjestelmäksi eri menetelmistä, elementeistä ja systemaattisista menettelyistä. Turvallisuusjohtamisjärjestelmä muodostuu useista osista, joiden tarkoitus on asettaa ja määrittää turvallisuustavoitteet, menetelmät tavoitteiden saavuttamiseksi, toimintatapavaatimukset ja seurantamenettelyt. Turvallisuusjohtamisjärjestelmä on johdon työväline ja keino toteuttaa turvallisuusjohtamista käytännössä. Turvallisuusjohtamisjärjestelmän keskeisin päämäärä on varmistaa, että onnettomuuksien ehkäisemiseksi ovat olemassa toimivat suojaukset ja niitä seurataan. (Levä 2003, 37 - 38.)

Kerkon (2001) mukaan turvallisuusjohtamisjärjestelmällä tarkoitetaan sellaista johdettua prosessia, joka huomioi organisaation kokonaisturvallisuuteen liittyvät asiat, on osa normaalia johtamista ja jota toteutetaan turvallisuuden näkökulmasta. Olennaista turvallisuusjohtamisjärjestelmässä on sen oikea sisältö ja tarvittavat ominaiselementit, joita ovat: johtamis-, järjestelmä- ja laadunhallintapiirteet. Hyvän turvallisuusjohtamisjärjestelmän sisällä on aina myös kokonaisturvallisuuden hallintajärjestelmä. Keskeisellä hallintajärjestelmällä tarkoitetaan, että turvallisuusasiat ovat esimerkiksi ohjeistettu ja päivitetty osana muuta dokumentaatiohallintaa. Dokumentointi on osa hallintajärjestelmäkokonaisuutta, jossa dokumentaatiot, ohjeet, oppaat, koulutukset ja tiedotukset, menettelytavat ja lainsäädäntövaatimukset on aukottomasti huomioitu ja joista vastaavat nimetyt henkilöt. (Kerko 2001, 22 - 23.)

Niemelä, Pirker ja Westerlund (2008, 117 - 119) määrittävät turvallisuusjohtamisjärjestelmän moniulotteiseksi kokonaisuudeksi, jolla organisaation strategian toteuttaminen mahdollistetaan käytännössä. Turvallisuusjohtamisjärjestelmä sisältää toimihenkilöille asetetut selkeät roolit ja vastuut, organisaatiossa vakiintuneet johtamistyylin ja kokouskulttuurin yhdistettynä tehokkaaseen viestintään, joka huomioi vaatimukset organisaation kehittämisessä ja muutosjohtamisessa. Ennen kaikkea hyvän johtamisjärjestelmän avulla on mahdollista kehittää organisaation toiminnan tehokkuutta monella tavalla, kuten esimerkiksi kehittämällä prosessien seuraamista, suunnittelua, ohjausta ja mittaamista.

Lainsäädännössä esitetyt turvallisuusjohtamisjärjestelmien vaatimukset ovat hyvin vaihtelevia. Tiettyjen toimialojen lainsäädäntö viittaa turvallisuusjohtamisjärjestelmän olemassaoloon ja jopa edellyttää sitä, mutta itse järjestelmän sisältövaatimuksia ei esitetä. Esimerkiksi työturvallisuuslaissa ei edellytä työnantajalta turvallisuusjohtamisjärjestelmän käyttöä, mutta lain toisessa luvussa esitetään myös sellaisia vaatimuksia, joita voidaan tulkita ja pitää sopivana turvallisuusjohtamisjärjestelmän olemassaoloa edellyttävänä vaatimuksena. Työsuojelun toimintaohjelma ja sen päivittäminen, riskien arvioinnin ajantasaisuus, riskianalyysin mukaiset toimintasuunnitelmat, työntekijöiden perehdyttämiset ja työympäristön jatkuva tarkkailu ovat juuri niitä ylläpidettäviä toimintoja, joita ilman selkeää ja koordinoitua järjestelmää ei pysty tehokkaasti toteuttamaan. (Työturvallisuuslaki 738/2002, 2 luku.)

Kansainväliset ISO ja OHSAS -standardit käsittelevät turvallisuuden hallintajärjestelmiä, joita Suomen standardoimisliitto SFS määrittelee johtamisen standardeiksi eli hallintajärjestelmästandardeiksi. Poikkeuksena on kuitenkin SFS-ISO 31000 riskienhallintastandardi, joka ei ole hallintajärjestelmästandardi. Hallintajärjestelmästandardeja on lukuisia ja niistä käytetyimmät ovat ISO 9001 laadunhallinta, ISO 14001 ympäristöjohtaminen ja OHSAS 18001 työterveys- ja työturvallisuusjohtaminen. Suomen standardoimisliiton tiedotteessa todetaan, että standardit merkitsevät organisaatiolle tehokkuutta, laatua, tuottavuutta ja kilpailukykyä. Hallintajärjestelmästandardien tavoitteena on saavuttaa parempaa toimintaa, joka on mahdollista

laadukkailla ja tehokkailla prosesseilla, turvallisilla toimintatavoilla, hyvällä ympäristöasioiden hoitamisella sekä riskien vähentämisellä. (SFS-tiedotus 2014, 2 - 9)

Ensimmäinen turvallisuusjohtamisjärjestelmä Suomessa perustui englantilaiseen sovellusohjeeseen työterveys- ja turvallisuusjohtamisjärjestelmästä BS-8800 ja hollantilaiseen Safety Checklist for Contractors (SCC) -standardiin. Suomessa BS8800 standardi korvattiin vuonna 2000 TTT-järjestelmällä, joka on työterveyden ja työturvallisuuden OHSAS 18001 spesifikaatio (The Occupational Health and Safety Assessment Series). (Levä 2003, 38 - 39.)

ISO 19011 on laadittu laadunhallinnan (ISO 9001) ja ympäristöjärjestelmän (ISO 14001) auditointiin ja se antaa lisäarvoa johtamisjärjestelmän arviointiin. ISO 19011 standardi ohjeistaa ja tarkastelee organisaatiossa käytössä olevien johtamisjärjestelmään sisältävien hallintajärjestelmien (ISO 9001 ja ISO 14001) arvioinnin suunnittelua, toteuttamista ja raportointia. Auditointistandardiin on myös lisätty tietojenkäsittelyä koskeva luottamuksellisuusperiaate. Auditointi ISO 19011standardissa on myös mahdollisuus etäauditointiin ja asetettu uusia auditointien pätevyysvaatimuksia. (SFS ry. 2015.) Molemmat (laatu ja ympäristöjärjestelmä) sisältävät jatkuvan kehittämisen mallin (PDCA -sykli tai kehämalli), joka on standardeissa käännetty ”Suunnittele / Plan, Toteuta / Do, Arvioi / Check, Toimi / Act”. (ISO 19011 2011, 16).

3.7 Auditointi

Auditoinnilla tarkoitetaan järjestelmällistä, riippumatonta ja dokumentoitua prosessia. Auditoinnissa hankitaan auditointinäyttöä, jonka perusteella arvioidaan objektiivisesti, täytyykö auditointikriteerit. Auditointikriteerit voivat olla politiikat, menettelyt tai vaatimukset, joihin auditointinäyttöä verrataan. Auditointinäyttöä ovat tallenteet, tositteet tai muu informaatio, jotka voidaan todeta liittyvän auditointikriteereihin. (ISO 19011 2011, 12). Auditoinnilla ei tarkoiteta prosessia, jossa pyrittäisiin etsimään näyttöä työntekijöiden epärehellisestä toiminnasta tai tekemistä virheistä tai horjuttaa työolosuhteita. Auditointi on tehokkaasti johdettu johdon työkalu, jonka tarkoituksena on esittää huolellisesti tallennettu, riippumaton ja totuudenmukainen kuva kohteen toiminnasta. Auditoinnin tulos on toteutettu puolueettoman ja tasapuolisen arvioinnin, täsmällisen tutkimuksen ja havainnoinnin avulla. Auditointinäyttö tulee perustua todellisuuteen, jossa puheet ja oletukset on poissuljettu. (Carter 2004, 56.)

Yleisesti sana ”auditointi” sekoitetaan ”katselmus” ja ”arviointi” sanojen merkitykseen (Carter 2004, 56). Katselmus määritetään toiminnoksi, jolla asian tilaa tutkitaan esimerkiksi selvittämällä, miten projekti etenee. (Moisiio ym. 2008, 11). Selvennykseksi ”katselmus” -termiä käytetään yleisesti johdon katselmuksien yhteydessä, joita toteuttavat yleensä yrityksen ylin johto. Johdon katselmuksessa käytetään hyödyksi auditoinneista saatuja tuloksia, joita sitten käytetään sisäisiin tarkoituksiin. Johdon katselmuksien, joita yleensä tehdään säännöllisesti

noin kerran vuodessa, päämääränä on hankkia tietoa esimerkiksi johtamisjärjestelmästä sen vaikuttavuuden varmistamiseksi tai parantamiseksi. (ISO 19011 2011, 12). Auditoinnin tarkoitus on objektiivisesti selvittää, vastaako käytäntö ja toiminto annettuja ohjeita, toimintamalleja ja standardeja. Auditoinnilla arvioidaan myös toimintojen tehokkuutta ja heikkouksia pyrkimällä löytämään kehittämiskohteita. (Green 1997, 25; Gray & Manson 2000, 17.)

Katakrin mukaisissa turvallisuusauditoinneissa korostuu auditoinnin ja auditoitavan kohteen vuorovaikutus. Ennen varsinaisia auditointihaastatteluita auditoinnin tulee etsiä vastauksia kysymyksiinsä dokumenteista ja asiakirjoista. Auditointiprosessin mukaisesti, auditoinnissa havaitut vakavat puutteet, tiedotetaan auditointikohteelle välittömästi korjaustoimien aloittamiseksi ja käynnistämiseksi. (Katakri II 2011, 4.)

Auditoinneista on esitetty useita myös muita tarkentavia määritelmiä. Auditointeja voivat olla ensimmäinen, toinen ja kolmas auditointi. Organisaation itse tai toimeksiantona suorittamat auditoinnit ovat sisäisiä auditointeja, joita kutsutaan myös ensimmäisen osapuolen auditoinneiksi. Toisen ja kolmannen osapuolen auditointeja kutsutaan ulkopuolisiksi auditoinneiksi, joissa toisen osapuolen edut liittyvät kohdeyritykseen, kuten asiakkaat tai heidän edustajat ja kolmatta osapuolta edustavat riippumattomat auditointiorganisaatiot, kuten sertifioivat tahot tai viranomaiset. (ISO 19011 2011, 12.) Auditoinnit voidaan luokitella myös muihin arviointitapahtumiin, kuten varsinaiseen ja vertaisauditointiin. Varsinaisella auditoinnilla tarkoitetaan Katakrin mukaisesti toteutettua koko auditointiprosessin läpikäyntiä, jota jatketaan kunnes esitetyt vaatimukset on täytetty. (Katakri II 2011, 4.) Vertaisauditoinnin idea on toteuttaa kahden erilaisen, mutta riittävän samankaltaisen, organisaation auditoinnit toisilleen. (Reiman ym. 2008, 343.)

Auditoinnista käytetään myös termejä esiauditointi ja seuranta auditointi. Esiauditoinnilla tarkoitetaan auditointia, jolla pyritään selvittämään, kuten tässäkin tutkimuksessa kohteen epävirallisena ja sisäisenä ensimmäisenä auditointina, kokonaisturvallisuuden nykytilaa ja tilannekuva sekä mahdollisesti valmentautua tulevaan varsinaiseen auditointiin. Seuranta-auditointi toteutetaan yleensä, kun kohde haluaa uusia sertifikaattinsa tai säännöllisesti todentaa, että kaikki todetut asiat edelleen täyttävät kriteeristön vaatimukset ja ovat käytössä. Auditoinneiksi on myös määritelty termit yhdistetty auditointi ja yhteisauditointi. Auditointia kutsutaan yhdistetyksi auditoinniksi, kun kohdeorganisaation kahta tai useampaa hallintajärjestelmää auditoidaan samanaikaisesti. Kun samaan kohdeorganisaatioon auditoi kaksi tai useampi auditointiorganisaatio, kutsutaan sitä yhteisauditoinniksi. (ISO 19011 2011, 12.)

4 Kansallinen turvallisuusauditointikriteeristö

Katakri on yhteistyössä puolustusministeriön, sisäasiainministeriön ja elinkeinoelämänkeskusliiton kanssa luotu kansallinen turvallisuuden auditointikriteeristö ja -malli. Katakriin tavoitteena on yhtenäistää viranomaistoimintoja, kun tehdään tarkastuksia sekä tukea ja varmistaa security -turvallisuuden toimivuus suomalaisissa yrityksissä ja organisaatioissa. Katakri valmistui osana Suomen hallituksen sisäisen turvallisuuden ohjelmaa 20.11.2009. Katakri mahdollistaa vastuuviranomaisten toiminnan läpinäkyvyyden ja yhtäläisyyden luomalla yhteinen kriteeristö turvallisuusauditointeihin. Kriteeristön tarkoitus on yhtenäistää turvallisuusmenettely omaavalvonnan ja auditoinnin parantamiseksi sekä yritysten että yhteisöjen turvallisuustason todentamiseksi. Katakri on työkalu varmistettaessa, että valtionhallinnolle palveluja tarjoava taho on kykenevä toimimaan turvallisuusluokitelluissa hankkeissa. (Katakri II 2011, 2.)

4.1 Katakri II

Katakri II versio keskittyy, turvallisuuden security -näkökulmaan (Katakri II 2011, 3). Suomen kielessä ”turvallisuus” -sanalle on annettu monia merkityksiä, joita Englannin kielessä kuvataan sanoilla joko safety tai security. Safety sanaa (turva, turvallisuus, varmuus, turvalaite, varmistin) käytetään, kun puhutaan onnettomuuksista ja niiden ehkäisemisestä sekä palo- ja pelastustoimista. Sanalla ”safety” tarkoitetaan myös usein fyysistä turvallisuutta, jossa henki tai terveys ei ole vaarassa, kuten työturvallisuus ja työsuojeluun liittyvissä toimissa. Security sanaa (turva, turvallisuus, turvatoimet, turvamiehet) käytetään, kun puhutaan poliisin väkivallan ja rikosten torjuntatoimista. Puheessa käytetyllä ”security” sanalla viitataan yleisesti kansainvälisellä tasolla yhteisöjen tai valtioiden turvallisuuteen. ”Security” sanalla viitataan myös esimerkiksi kulunvalvontaan ja erityisesti tietoturvaan ja tiedon suojaamiseen. (Hanén 2005, 20 - 21.) Katakriin päätavoitteena on siis varmistaa, ehdottomina pidettyjen vaatimuskriteereiden täyttämisen todentamisella, että suojattavaksi luokitellut salatut tiedot säilyttävät käytettävyyden, luotettavuuden sekä eheyden ja pysyvät silti salassa. (Katakri II 2011, 3.)

Katakriilla varmistetaan, että viranomaisten luokitteleman salattavan tiedon käsittely, kaikissa olosuhteissa on kriteeristön mukaisesti, turvallisesti ja luotettavasti toteutettu. Katakriin päätavoitteen mukaan luotiin viranomaisille yhtenevä käytäntö ja auditointimenettely kohteen turvallisuustason todentamiseksi. Kun kohteessa tehtävä tarkastus, auditointi toteutetaan, suomalaiselta yritykseltä tai muulta yhteisöltä vaaditaan silloin yksityiskohtaista suojaustasovaatimuksen täyttämistä. Katakri toimii kohteen turvallisuustason varmentamisessa velvoittavana kriteeristönä, kun turvallisuustodistusta haetaan. Kriteeristöllä pyritään siihen, että toteutettavassa auditointiprosessissa otetaan kaikkien osa-alueiden vaatimukset huomioon. Ehdottoman vaatimuksen taustalla on ollut pyrkimys, ettei auditoinnin jälkeen jää tunnistamattomia tai kriittisiä riskejä. (Katakri II 2011, 3.)

Kriteeristön tavoitteena on myös auttaa yrityksiä oman turvallisuustyön ja -toiminnan määrittämisessä. Kriteeristöissä on esitetty, viranomaistasovaatimusten lisäksi, elinkeinoelämän yleissuosituksia (EK:n suositustaso). Elinkeinoelämän suosituksista voi löytää käyttökelpoisia turvallisuutta parantavia käytäntöjä turvallisuusjohtamisen alalla ja niiden avulla voi tarvittaessa kehittää turvallisuutta aina viranomaistasovaatimuksien tasolle asti. Juuri näitä kriteeristön ominaisuuksia hyödynnetään tässä tutkimuksessa ja auditoinnissa. (Katakri II 2011, 3.)

Viranomaistasovaatimukset on luokiteltu kolmiportaiseksi vastaten valtionhallinnon tietoturvallisuusasetuksen mukaista käsitteistöä: perustaso (IV), korotettu taso (III) ja korkea taso (II). Katakri koostuu neljästä eri turvallisuuskokonaisuuden pääosan alueesta, joita ovat: A: Hallinnollinen turvallisuus (turvallisuusjohtaminen), P: Henkilöstöturvallisuus, F: Fyysinen turvallisuus ja I: Tietoturvallisuus. (Katakri II 2011, 3, 7.)

4.2 Katakri 2015

Katakri 2015 päivitystulos julkaistiin keväällä 2015, pdf tiedostoversiona otsikolla ”Tietoturvallisuuden auditointityökalu viranomaisille”. Tämä 71 -sivuinen uusi malliversio on jaettu kolmeen osa-alueeseen. Osa-alueet on nimetty seuraavasti: T: Turvallisuusjohtaminen, F: Fyysinen turvallisuus ja I: Tekninen tietoturvallisuus. Turvallisuusjohtamisen osa-alue on jaettu kahteen alaosaan: Hallinnolliseen turvallisuuteen ja Henkilöstöturvallisuuteen. Fyysinen turvallisuus on jaettu neljään alaosaan: Tiloja ja laitteita koskevat vaatimukset, Luvattoman pääsyn estäminen, Suojaaminen salakatselulta ja salakuuntelulta ja Toiminnan jatkuvuuden hallinta. Tekninen tietoturvallisuus on jaettu neljään alaosaan: Tietoliikenneturvallisuus, Tietojärjestelmäturvallisuus, Tietoaineistoturvallisuus ja Käyttöturvallisuus. (Katakri 2015, 4 - 5.)

Koska Katakri 2015 on nimen mukaisesti viranomaisille osoitettu työkalu, on (T) osa-alueessa kuvattu turvallisuusjohtamisen vähimmäistaso, jonka yrityksen on valmiudeltaan ja kyvykkyydeltään aina täytettävä. Fyysisen turvallisuuden (F) osa-alueessa on kuvattu, miten turvallisuusvaatimukset täytetään salassa pidettävien tietojen osalta fyysisessä käyttöympäristössä. Salassa pidettävien tietojen mukaan suojattavat kohteen tilat jaetaan käsittely- ja säilyttämistarpeen mukaan kolmeen alueeseen: hallinnolliseen alueeseen, turva-alueeseen ja tekniseen turva-alueeseen. Teknisen tietoturvallisuuden (I) osa-alueessa esitetään asetetut turvallisuusvaatimukset tekniselle tietojenkäsittely-ympäristölle ja ne jakautuvat kolmeen suojaustasoon: perustaso (ST IV), korotettu taso (ST III) ja korkea taso (ST II). (Katakri 2015, 4 - 5.)

Edeltäjänsä nähden Katakri 2015 ei ole enää mikään päivitys vaan täysin uusi malli tai versio kriteeristöistä, sillä muutokset ovat sen verran merkittäviä. Vaatimusten lukumäärää on vähennetty aiemmasta 160:stä reiluun 40:n ja suojaustasokohtaiset vaatimukset on yhtä osiota lukuun ottamatta poistettu. Merkittävin muutos aikaisempaan on, että Katakri 2015 on riski-

lähtöinen ja riskien arvioinnista on tehty pakollinen vaatimus. Suojattavan kohteen ja kyseisen kohteen suojausluokitus sekä tiedon käsittely-ympäristö että mahdolliset uhat vaikuttavat riskiarvioon. Nyt uudessa Katakri versiossa aloitetaan ensin työskentely riskiarvioinnin tekemisellä ja vasta sitten suojattavien kohteiden vaatimuksia tulkitaan tehdyn riskiarvion perusteella. Uudella lähestymiskulmalla mahdollistetaan yrityksen uhkatason huomioimisen suunniteltaessa toteutettavia kontroleja ja suojausratkaisuja. Rakenteeltaan muuttunut uusi Katakri mahdollistaa myös yritysturvallisuuspalvelusten osittaisen toteuttamisen.

4.3 Auditointiohjelma ja toteutus

Tämän tutkimuksen tavoitteena oli kartoittaa kohteen hallinnollisen turvallisuuden nykytila ja taso sekä tulosten perusteella laatia kehittämisehdotusraportti. Tavoitteeseen pääsemiseksi valittiin työvälineeksi kansallinen turvallisuusauditointikriteeristö Katakri. Katakriin avulla pyrittiin tekemään sellainen auditointiohjelman mukainen esiauditointi, joka auttoi löytämään, tunnistamaan ja priorisoimaan mahdolliset kohdeyrityksen kokonaisturvallisuuden ja turvallisuusjohtamisen kehittämiskohteet. Toisena tavoitteena oli saada selville, miten Katakri soveltuu kyseisen kohdeorganisaation kokonaisturvallisuuden auditointi- ja kehittämisvälineeksi.

Katakriin ominaispiirteen mukaista varsinaista turvallisuusauditointia ei toteutettu tässä tutkimuksessa, koska silloin se olisi tarkoittanut, että auditointiprosessia olisi jatkettu niin kauan kunnes kaikki kriteeristön vaatimukset olisi täytetty. Tarkoituksena ei ollut myöskään valmistaa kohdetta varsinaiselle auditoinnille, koska mitään sellaista tarvetta ei sillä hetkellä ollut eikä tavoitteeksi asetettu saavuttaa hyväksytyt ja vaatimukset täyttävä viranomaisten myöntämä todistus. Edellä mainituista syistä tämä tutkimus toteutettiin käyttämällä Katakriin kriteeristöä rajatusti ja auditointiprosessia sovellettiin vain osin. Katakriin auditointiprosessi loi kuitenkin peruslähtökohdan, jonka pohjalta auditointiohjelma rakennettiin ja toteutettiin.

Katakri II:n mukaan auditointiprosessi etenee siten, että ennen varsinaisen auditoinnin aloittamista, tehdään etukäteen pikainen dokumentaatioanalyysi kohdeorganisaatiosta. Auditoinnin tulisi siten pystyä prosessin mukaan, saamastaan kohdeorganisaation yleistilanteesta, luomaan riittävä tilannekuva, jonka perusteella pystytään esittämään tarvittava dokumentaatioiden toivelista. Tämä ei ole kronologisesti mahdollista, sillä Katakri ei esitä suoraan vaadittavaa kriteeristön mukaista asiakirjalistaa, jonka mukaan auditoinnin alussa voitaisiin pyytää tarkastettavaksi ja tutkittavaksi oikeat tarvittavat dokumentaatiot. Onnistuakseen tässä auditointiprosessissa auditoinnin on samalla, kun tutustuu organisaation toimintaan, myös perehdyttävä kriteeristön vaatimuksiin eli esitettäviin kysymyksiin. Vasta perehtymisen perusteella voi auditoinnin eriyttää ja tulkita kriteeristön mukaisia vaatimuksia siten, että tarvittavien dokumentaatioiden lista voidaan laatia ja esittää. Kriteeristön asiakysymyksiin perehtymisen yhteydessä tulee tarpeelliset dokumentit ja kysymykset laadittua samanaikaisesti, jolloin en-

nen auditointia on jo esitetty ne kysymykset, joita esitetään myös ensimmäisessä eli varsinaisessa auditoinnissa. Tämä kronologiaongelma häviää ammattilaiselta ja auditointiasiantuntijalta, kun auditointi on suorittanut useita auditointiohjelmia, koska auditointi on jo rakentanut dokumentaatioista tarvittavat toivelistat, jotka voidaan heti kohteen yleistilanteen hahmottamis- ja perehtymisvaiheessa suoraan antaa kohdeorganisaation yhteyshenkilölle.

Reimanin ja Oedewaldin (2008, 344) mukaan dokumenttien ja asiakirjojen suora tarkastelu ei aina paljasta organisaatiossa kyteviä tai havaitsemattomia vaaroja. Dokumenttien olemassaololla ei myöskään pysty aukottomasti osoittamaan, miten organisaatiossa todella käytännössä toimitaan tai ylläpidetään ja hallintaan turvallisuutta. Tästä syystä myös Katakri II:n auditointiprosessi tähdentää, että auditoinneissa vuorovaikutus auditoinnin ja auditoitavan kohteen välillä korostuu. Jotta auditointi ei jäisi yksinomaan asiakirjojen tarkastelun tasolle, on dokumentaatiovaiheen jälkeen, tehtävä suunnitelma tarkastettavista tai kierrettävistä kohteista, joita auditoidaan. Auditointiprosessista saadut tulokset kirjataan ylös, jonka perusteella tehdään arviot vaatimusten täyttymisestä ja poikkeamista tai puutteista. Mikäli jotain Katakriin kriteeristön mukaista suojaustasoa kohde ei pysty täyttämään, auditoitavan kohteen tulee osoittaa jokin muu korvaava tai riittävä turvallisuusmenettely. Auditoinnista annetaan kohteelle auditoinnin päätyttyä kirjallinen raportti. (Katakri II 2011, 4.)

Suunniteltu ja asiakkaan hyväksymä auditointiohjelma perustui kohdeorganisaatiosta saatuihin etukäteistietoihin. Auditointiohjelman perusrunko rakentui kriteeristön mukaisesti esitettyihin sekä niistä johdettuihin kysymyksiin. Kysymykset muokattiin kohdeorganisaatiolle sopivammiksi ja niitä esikäsiteltiin siten, että saatiin luotua etukäteen sellaiset toivelistat, joiden mukaan pystyttäisiin tekemään vaaditut päätelmät kriteeristön täyttymisestä. Laaditut listat sisälsivät auditoinnissa tarkasteltavaksi halutut dokumentit ja tiedot kohdeorganisaatiossa tehdyistä turvallisuustoiminnoista sekä kysymyksistä, joihin toivottiin saavan vastauksia. Tarkoituksena oli toteuttaa ensin dokumentaatioiden tarkastelu, joiden perusteella esitettäisiin haastattelukysymykset johdolle. Periaatteena oli, että ”esitä dokumentti tai selitä”, joita sitten myöhemmin kokonaiskuvan mukaan analysoitiin. Esimiehistöille voitiin avata laaditut kysymykset samanaikaisesti, koska kysymykset oli muokattu etukäteen, jotta voitiin rationaalisesti kohdentaa kaikille osapuolille tiedonkeruumenetelmiä ajallisesti tehokkaasti. Kaikissa vaiheissa ja tilanteen eläessä oli tarkoitus myös tehdä havaintoja johtopäätösten tueksi.

Tässä opinnäytetyössä käytettiin auditoitavaan kohteeseen Katakriin kriteeristössä hallinnollisen turvallisuudesta esitettyjä EK:n suositustason mukaisia (versio II) tai perustason (versio 2015) kysymyksiä. Hallinnollisella turvallisuuden kysymyssarjalla todennettiin vertailemalla turvallisuusjohtamisen taso ja toimivuus. Työssä selvitettiin kohdeyrityksen kokonaisturvallisuuden nykytilanne, joka toteutettiin esittämällä kysymyksiä. Eri tavoin saatuja ja kerättyjä haastatteluiden ja kyselyiden vastaustietoja analysoitiin ja täydennettiin havainnoinnilla.

Tavoitteen saavuttamiseksi, auditoinnin toteuttamiseksi ja tulosten vertailuarvioinnissa käytettiin apuna Katakryn kriteeristössä esitettyjä kysymyksiä:

- Auditointimalli räätälöitiin kohdeorganisaation tarpeita vastaavaksi, koska yritys ei ole turvallisuuskriittinen toimija eikä pakottavaa tarvetta kriteeristön täytölle ole.
- Auditointimallin kysymyksiä muokattiin kohdeorganisaation toimintaa vastaavaksi, jotta kysymyksillä pystyttiin paremmin saamaan kysytyt asiat esille ja kartoitettua nykytila.

Auditoinnin toteutustyössä syntyi kartoitusten, havaintojen ja analysointien tuloksina saadut tiedot, arviot ja huomiot, joiden mukaan laadittiin kohdeyrityksen turvallisuuteen liittyvistä puutteellisuuksista kertova kehittämisehdotusraportti. Auditoinnista saatujen kokemusten perusteella selvitettiin ja arvioitiin myös toista tämän työn tavoitetta eli Katakryn soveltuvuutta kohdeorganisaation turvallisuusauditointeihin sekä työväliseen käyttökelpoisuutta kun kokonaisturvallisuutta halutaan tulevaisuudessa vielä parantaa ja kehittää lisää.

5 Empiirinen tutkimusasetelma

Empirismi tarkoittaa, että tutkimusta koskeva tieto perustuu todelliseen kokemukseen ja havaintoihin sekä määritelmä korostaa kokemuksen merkitystä tai pitäytymistä aistivaikutelmiin sekä tosiasioihin, mutta jäsentää tietoa logiikan ja matematiikan tarjoamin keinoin. (Koppa 2015.) Empiiristä tutkimustietoa tarvitaan toimintamekanismien ymmärtämiseksi paremmin. Empiirisen tutkimuksen tehtävä on tietojen hankkiminen päätöksen teon perustaksi. Empiirisen tiedon hyödyntäminen lisää toimivuutta ja tehokkuutta eli käytännön selvityksellä vähennetään päätöksentekoon liittyvää epävarmuutta löytämällä tutkittavasta ilmiöstä säännönmukaisia tekijöitä. Todellisuuden tunteminen ja totuudenmukainen kuvaaminen on tärkeää, jotta oikeasuhteisuus yleistyksissä ja selittämisessä olisi mahdollista. (Lanne 2007, 25.)

Tässä tutkimuksessa pyritään toimeksiannon perusteella löytämään kohdeorganisaation hallinnollisesta turvallisuudesta kehittämiskohteita. Tämä tutkimus lähtee olettamuksesta, että vaaditut kehityskohteet löydetään toteuttamalla kohdeorganisaatiossa turvallisuusauditointi. Auditoinnista odotetaan saavan riittävästi tietoja perehtymällä yrityksen turvallisuudesta tehtyihin dokumentteihin, toteuttamalla kyselyjä ja haastatteluita sekä kaikista tiedoista tehtävillä analysoinneilla ja havainnoilla. Tutkimus lähtee ajatuksesta, että vertaamalla nykytilanetta asetettuun vaatimustasoon saadaan auditointitulokset, jonka mukaan voidaan todentaa turvallisuuspuutteet. Puutelistan perusteella pystytään laatimaan kohdeorganisaation tilaama raportti, jossa on asetettu priorisoituna kokonaisturvallisuuteen liittyvät kehittämiskohteet ja ehdotukset turvallisuuden kehittämisen jatkotoimenpiteistä.

5.1 Tutkimusote ja toimintatavat

Tämä opinnäytetyö on strategialtaan laadullinen tapaustutkimus, jonka tavoitteena oli tunnistaa ja määrittää yrityksen X hallinnollisen turvallisuuden puutteet ja kehittämiskohteet. Tutkimuksen tarkoitus on aluksi kartoittava ja lopuksi selittävä, sillä Hirsjärven ym. (2008, 134) mukaan tutkimus voi sisältää useampia tarkoituksia ja tutkimuspiirteet voivat myös muuttua tutkimuksen aikana. Kartoittavalla osuudella tutkimus pyrkii selvittämään, mitä nyt tapahtuu tai mitä ei ole tehty ja katselmoimalla tutkimuskysymyksen mukaisia turvallisuuspuutteita. Selittävässä osuudessa tutkimuksessa pyritään etsimään selitystä kausaalisuuksien kautta nykytilanteelle, jotta esitettävät kehitysehdotukset olisi perustellumpia kuin tulokset.

Tämä tutkimus lähtee security -turvallisuuden lähtökohdista tutkimaan organisaation hallinnollista turvallisuutta. Security sana turvallisuus tarkoittaa, Katakriin näkökulmasta, tiedon turvaamista ja suojaamista, jota ylläpidetään valvomalla sekä varmistamalla ja varautumalla turvallisuuspoikkeamatilanteiden varalle. Tutkimustyön tavoitteita perustellaan kohdeorganisaation asettamien kehittämistoimien tarpeellisuudella. Opinnäytetyön tavoitteena on tunnistaa, määrittää ja kehittää kohdeyrityksen kokonaisturvallisuutta hallinnollisesta turvallisuudesta löytyneiden puutteellisuuksien kautta. Kartoituksen tarkoitus on tuottaa arviointi, jolla luodaan pohja laajemmalle kokonaisturvallisuuden kehittämistoiminnalle lähitulevaisuudessa. Lähtötilakatselmus tai auditointiohjelma on kuin mikä tahansa projekti, joka tehdään ja toteutetaan tarkan suunnitelman mukaan johdon valvonnassa muistaen, että kysymyksessä on alkutoimenpide, jonka jälkeen varsinainen kehittämistyö vasta alkaa (Kerko 2001, 40).

Kartoitus suoritettiin käyttämällä hyväksi Katakri II ja Katakri 2015 turvallisuuskriteeristössä esitettyjä kysymyksiä vertailuarvoina nykytilanteen todentamiseen. Kohdeyrityksen nykytilaa verrattiin Katakri II:ssä esitettyyn, elinkeinoelämän suositukset (EK:n), mukaiseen tavoitetasoon. Katakri 2015:a ei ollut eriteltävissä tasovaatimuksia, jonka johdosta kriteerinä käytettiin kriteeristössä esitettyä perustasoa. Arviointitulosten käsittelyssä käytettiin kolmiportaista poikkeamajaottelua helpottaakseen kehittämiskohteiden analysointia ja priorisointia. Nykytilan vertailussa käytettävää asteikkoa on avattu tarkemmin luvun 6 alussa.

Koska Katakriin mukainen kriteeristön vertailuosuus kohdistettiin ainoastaan hallinnollisen turvallisuuden osa-alueisiin eli turvallisuusjohtamiseen, tutkimusta ohjaa ajatus, että kaikki turvallisuudessa havaitut puutteet johtuvat juuri organisaatiossa havaitusta turvallisuuskulttuurista, toimintatavoista, menettelytavoista tai ovat seurausta puutteellisesta turvallisuusjohtamisesta. Turvallisuuden auditoinnissa käytettiin apuvälineenä kansallista turvallisuusauditointikriteeristöä Katakria. Auditoinnin toteuttamiseksi Katakrista käytettiin hyödyksi auditointiprosessin kuvausta, auditointiohjelman ohjeita ja kriteeristössä esitettyjä kysymyksiä. Kriteeristön kysymyksiä pyrittiin muokkaamaan kohdeorganisaation kohdejoukon mukaan.

5.2 Tiedonkeruu- ja analysointimenetelmät

Tässä alaluvussa kerrotaan, miten ja milloin tiedonkeruuta eri menetelmin toteutettiin. Samalla pyritään perustelemaan menetelmien valintaa ja tarkoitusta, miksi kyseistä tiedonkeruumenetelmään käytettiin. Tässä kvalitatiivisessa tutkimuksessa ja auditoinnissa käytettiin useita erilaisia tiedonkeruumenetelmiä. Tiedonkeruun primääriaineiston muodostivat dokumentaatiot, strukturoidut kirjalliset kyselyt ja teemahaastattelut. Sekundäärisen aineiston muodostivat strukturoidusta turvallisuuskyselystä saadut vastaukset ja havainnoinnin tulokset. Koska esitetyt tiedonkeruumenetelmät ovat hyvin käytettyjä, ne ovat myös tehokkaita tapoja kerätä laadukasta tietoa vastaavanlaisten kehitystehtävien määrittelemiseksi.

5.2.1 Dokumenttianalyysi

Kvalitatiivinen tutkimus on lisännyt tiedonkeruutapoja, joilla pyritään ymmärtämään toimijoi- ta heidän tuottamiensa dokumenttien kautta. Dokumenttiaineiston analysoinnissa aineistoon on suhtauduttava kriittisesti ja luotettavuutta on myös tarkoin punnittava. Dokumentti- analyysillä tarkastellaan kohteesta löydettäviä valmiita aineistoja, joita ovat turvallisuusdo- kumentaatiot ja asiakirjat. Koska kohdeorganisaation dokumentit ja asiakirjat sisältävät väli- töntä tietoa, kutsutaan niitä primääriaineistoksi. Vertailukelpoisuuden saamiseksi tietoja on kuitenkin muokattava, normitettava ja yhdisteltävä. (Hirsjärvi ym. 2009, 189, 212.)

Dokumentaatioanalyysin valintaa yhdeksi tiedonkeruumenetelmäksi perustellaan Katakriissa esitetyn turvallisuusauditointiprosessin teknisestä suorituksista tehdyn toteutusohjeen mukai- sella toiminnalla ja dokumentaatiopohjaisella tilanteenarvioinnin tärkeydellä (Katakri II 2011, 5). Tässä tutkimuksessa kerättiin Katakriin auditointikriteeristöä kysymysvaatimusten mukai- sesti tarvittava dokumentaatiolista, joka esitettiin pyyntönä kohdeorganisaation vastuuhenkilöille. Saatujen ja todennettujen dokumentaatioiden sisältöjä verrattiin kirteeristöä asetet- tuihin tavoitetasoihin. Saatujen tulosten perusteella tehtiin arviot kriteereiden täyttymisestä vasta sen jälkeen, kun kaikki muut auditoinnin tiedonkeruusuudet oli toteutettu. Dokumen- taatioanalyysi perustui siten vain osaltaan Katakrista saatuun vertailukriteeristöön.

Dokumentteihin tutustumiset aloitettiin jo kesäkuussa, kun pyrittiin saamaan selkoa yrityksen tekemistä turvallisuusjärjestelyistä sekä hahmottamaan kohteen kokonaiskuvaa. Kohteeseen perehtymisen aikana määriteltiin myös kehittämisen tavoitteita ja rajauksia. Perehtymistä jatkettiin suunnitelman mukaan aina elokuun alkuun asti. Turvallisuuteen liittyviä dokumen- teja ja asiakirjoja pyydettiin johtajistolta koko auditointiprosessin ajan eli syyskuun loppuun saakka ja dokumentteja saatiin analysoitaviksi yhteensä 32 kappaletta.

5.2.2 Haastattelu

Haastattelu on vaativa tiedonkeruumuoto jota ei tule valita perustelematta ja sen on sovellettava kyseisen ongelman ratkaisuun. Tiedonkeruun päämenetelmänä haastattelu soveltuu tähän kvalitatiiviseen tutkimuksen osaan. Haastattelun valintaa puoltavat perustelut, että haastattelussa saatuja vastauksia voidaan selventää ja syventää sekä niihin voidaan myöhemmin palata sekä vastauksia täydentää. Haastattelut ovat myös tässä tutkimuksessa perusteltuja, koska samanaikaisesti voidaan toteuttaa havainnointia. Haastattelujen etuna on myös, että niitä voi säädellä joustavasti tilanteen ja haastateltavan mukaan.

Tässä tutkimuksessa käytettiin tiedonkeruumenetelmänä teemahaastattelua. Tyypillisen teemahaastattelun mukaan haastattelun aihepiiri oli haastateltaville tiedossa, koska etukäteen pyydettiin perehtymään aihealueesta annettuihin kysymyksiin, joita oli työnkuvausten ja vastuujon periaatteen mukaisesti räätälöity sekä lähetetty kullekin johtajalle erikseen. Teemahaastattelun valintaa tiedonkeruumenetelmänä ja käyttöä perustellaan sillä, että dokumentteihin tutustumalla ei saada riittävää tietoa, miten todella asiat hoidettu tai ovat järjestettyjä sekä onko dokumentaatiot vain laadittu ja tehty arkistoitavaksi paperimassaksi.

Haastatteluiden järjestäminen ei ole ongelmatonta, sillä heikkoutena ovat aikataululliset syyt, koska haastatteluihin kuluu aikaa ja ne vaativat huolellisen suunnittelun. Haastattelutulojen luotettavuutta saattaa myös heikentää taipumus antaa sosiaalisesti suotavia tai tilanteeseen sopivia vastauksia. Samalla haastatteluaineiston analysoinnissa on koettu ongelmaksi, että haastattelutilanne on hyvin konteksti ja tilannesidonnainen ja haastateltava saattaa puhua ja vastata toisin kuin jossakin toisessa tilanteessa vastaisi. Tässä tutkimuksessa haastatteluissa käytettävät kysymykset laadittiin Katakrista saatavista vaatimuskriteereistä. Tavoitteena haastattelukysymyksillä oli täydentää aikaisempaa kirjallista strukturoitua kyselyä ja saada ensikäden tietoa suoraan haastateltavilta sellaisiin kysymyksiin, joiden moniselitteisyys tai monimutkaisuus ei muutoin olisi avautunut. (Hirsjärvi ym.2009, 199 - 203.)

Tutkimusaineistoa on hyvä koota haastatteleamalla, jos tutkimuksen yhtenä tavoitteena on tuottaa tietoa asenteista, arvoista, mielipiteistä, käsityksistä, havainnoista tai kokemuksista. (Koppa 2015. Haastattelut.) Teemahaastattelulla tarkoitetaan, Tilastokeskuksen mukaan, että kerättävä aineisto kertyy haastateltavan kokemuksista. Tutkimuksessa ei varsinaisesti tutkita todellisuutta vaan, miten haastateltava näkee todellisuuden. Vaikka etukäteen on suunniteltu tutkimusongelman ratkaisemiseksi valitut teemat ja vastausvaihtoehdot, nämä eivät rajaa kertyvää aineistoa vaan itse haastattelussa saattaa ilmetä mitä vain. (Kurkela, R 2015.)

Yrityksen johtajiston haastattelut toteutettiin elokuun puolesta välistä syyskuun alkuun asti, jolloin haastateltiin yrityksen liiketoiminta-, henkilöstö- ja kahta palvelujohtajaa. Ylimmälle

johdolle oli, esiselvitysten perusteella ja saatujen työnkuvien mukaan, laadittu vastuualueiden mukaisesti kohdennettuja 42 - 46 kysymyksen sarjoja, joihin tuli vastata kirjallisesti. Kysymyssarjat lähetettiin perehtymistä varten ennen varsinaisia haastatteluja. Kysymyksiä täydennettiin ja käsiteltiin tarkemmin kohdennetuilla henkilökohtaisilla teemahaastatteluilla. Haastatteluista saadut tiedot edustivat siten myös merkityksellisintä osaa koko auditointiprosessissa ja haastattelutiedot tukivat selkeästi jo dokumentaatioista tehtyjä ennako arvioita.

5.2.3 Kysely

Yksi tapa kerätä tutkimusaineistoa on toteuttaa kysely, jossa vastaajiksi valitut kohdehenkilöt muodostavat otoksen tietystä perusjoukosta. Kyselyn aineistoa yleensä käsitellään ja analysoidaan kvantitatiivisin menetelmin eli tulkitsemalla vastauksina saatuja numeraalitietoja. Menettelyn etuna on tehokkuus, nopeus ja vaivattomuus, mutta heikkoutena yleensä vastausprosentin alhaisuus. (Hirsjärvi ym.2009, 188 - 190.) Kyselyn strukturoinnilla tarkoitetaan, Tilastokeskuksen mukaan, että kysymykset ovat niin tarkoin harkittuja, että sekä kysymys että vastausvaruus on ennalta annettu ja suljettu. (Kurkela 2015.)

Hirsjärven ym.(2009, 190) mukaan kyselyyn liittyy suuria heikkouksia. Kyselyn toteutuksessa ja siihen tehdyissä vastauksissa ei ole mahdollista varmistua, miten vakavasti kyselyyn on suhtauduttu. Kyselyssä ei voida tietää, miten hyvin vastaajat ovat perehtyneet aihealueeseen tai selvillä esitettävistä kysymyksistä. Kyselyn heikkoutena pidetään myös, että väärinymmärryksiltä ei voida välttyä, koska kyselyn onnistuminen on kiinni annetuista vaihtoehdoista ja vastaajien omasta näkökulmasta. Kunnollisen, selkeän ja vastauksiltaan luotettavan kyselylomakkeen laatiminen vaatii paljon aikaa sekä testaamisvaiheessa että muokkaamisvaiheessa.

Auditoinnin aikana järjestettiin muun tiedonkeruun tueksi vielä kvantitatiivinen, yrityksen esimiehistöille osoitettu, strukturoitu 101 kysymyksen turvallisuuskysely verkon kautta toteutettuna. Esimiehistöä turvallisuuskyselyyn vastasi yhteensä 45 henkilöä 53:sta (85 %). Yrityksen ylimmälle johdolle toteutettiin vastaava, mutta laajempi 141 kysymyksen kysely, joka oli eri kuin kirjallisesti tehty kysely ja johon vastasi kaikki 4 henkilöä. Turvallisuuskyselyt toteutettiin 17.8. - 18.9.2015 välisenä aikana ja kokonaisvastausprosentiksi kyselyille saatiin 86 prosenttia, jota voidaan pitää olosuhteisiin ja kyselyaikaan nähden erittäin hyvänä tuloksena.

Perusteena kyselyiden valintaan yhdeksi auditoinnin tiedonkeruumenetelmäksi oli, että nopeampaa tapaa ei ole, jolla voitaisiin saada käyttökelpoista ja suuntaa antavaa tietoa kohteesta ja tutkittavasta sekä kysytystä asiasta. Kvantitatiivisten kysymysten tarkoitus oli kartoittaa kohdeorganisaation turvallisuusasioiden ympärillä vallitsevaa ymmärtämystä, toimintatapakulttuuria, mielikuvia ja tuntemuksia. Kyselyn periaatteena oli saada aikaan kysytyille asioille ja aiheille selkeä laskennallinen matemaattinen paremmuusjärjestys, jota voidaan arvioida ja

analysoida dokumentaatioiden, haastatteluiden ja havaintojen mukaan samanaikaisesti vertailemalla. Kyselyssä kartoitettiin, kriteeristön mukaisesti, oliko kohdeorganisaatiossa vaaditut toiminnot tai toimenpiteet suoritettu tai toiminnassa. Katakriassa esitetyt kysymykset sisällysivät useita alakysymyksiä tai aihealueita, jotka kysymysten ymmärrettävyyden vuoksi tai selvyyden parantamiseksi pilkottiin erillisiksi kysymyksiksi. Samalla Katakriin kysymyksistä useita oli myös yhdistettävissä, koska samoja asioita tai aiheita kysyttiin useammassa kohdassa.

Tämän tutkimuksen asettamat tavoitteet kyselylle oli saada aikaan selkeä vertailuero ja skaalautuvuus kysytyjen kriteerien välille. Kyselyn tavoitteena oli selvittää ja todentaa, mitä turvallisuustoimenpiteitä mielletään tehdyiksi tai tekemättömiksi, onko asiasta mitään tunnettua tietoa sekä kuinka merkityksellisinä kyseisiä toimia pidetään kohdeorganisaatiossa. Strukturoitu kysely laadittiin Likertin 0 - 5 arvoasteikolla, joissa kaikissa oli samat väittämien vastausvaihtoehdot. Vastausvaihtoehtoina olivat: 0 = En osaa sanoa, 1 = Täysin eri mieltä, 2 = Eri mieltä, 3 = Melko samaa mieltä, 4 = Samaa mieltä, 5 = Täysin samaa mieltä. Kysymykset laadittiin Katakri II ja Katakri 2015 hallinnollisen turvallisuuden kriteeristön mukaisesti laadittujen tavoitetasojen mukaisesti. Kysymyksiä oli 10 ja kysymysten yhteismäärä 70. Kysymysmäärät on esitelty myös taulukossa 1, arviointitulosten esittelyluvussa 6.1.

Katakri II (2011, 7) hallinnollisen turvallisuuden pääalueiden mukaiset kysymysmäärät:

- A100 (9 kpl:ta) Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt
- A200 (4 kpl:ta) Turvallisuuden vuotuinen toimintaohjelma
- A300 (6 kpl:ta) Turvallisuuden tavoitteiden määrittely
- A400 (12 kpl:ta) Riskien tunnistus, arviointi ja kontrollit
- A500 (7 kpl:ta) Turvallisuusorganisaatio ja vastuut
- A600 (8 kpl:ta) Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet
- A700 (4 kpl:ta) Turvallisuusdokumentaatio ja sen hallinta
- A800 (8 kpl:ta) Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen
- A900 (5 kpl:ta) Raportointi ja johdon katselmukset

Katakri 2015 (2015, 2 & 6) hallinnollisen turvallisuuden ja turvallisuusjohtamisen osa-alueiden kysymysmäärät T 01 - T 07 (7 kpl:ta).

Kvantitatiivisen kyselyn tulokset myötäilivät pääsääntöisesti samoja tuloksia, joita Katakriin mukaan tehdystä auditointiarviostakin saatiin. Kysymysten mukaan oli muutamia osa-alueita, joiden tuloksissa ilmeni suuria heittoja kyselyn ja poikkeama-arvion välillä. Tämä on kyselystä saatujen palautteiden mukaan johtunut siitä, että auditoija ei ole osannut muokata kysymyksiä riittävän ymmärrettävään muotoon, jotta olisi osattu vastata ”oikein”. Poikkeavissa tapa-

uksissa on käytetty aina kriteeristön mukaisesti saatua poikkeama-arviotulosta kyselyn sijaan. Turvallisuuskyselyistä saatujen vastauksien tulokset on esitetty liite osiossa viimeisenä.

5.2.4 Havainnointi

Tutkija saa kyselyllä ja haastattelulla selville, mitä vastaajat ajattelevat, uskovat tai tuntevat. Menetelmät kertovat sen, mitä kohderyhmä itse pääättelee ja havaitsee ympäristöjensä tapahtumista. Ne eivät kuitenkaan kerro, mitä todella tapahtuu tai toimitaanko oikeasti juuri niin kuin, kyselyyn tai haastatteluun, on vastattu. (Hirsjärvi ym.2009, 207.) Tästä syystä on tutkimuksen tekijän tekemät paikan päällä tehdyt havainnot myös tärkeitä tiedonlähteitä. Havainnoinnin valintaa tiedonkeruumenetelmänä perustellaan juuri autenttisesti saatujen lisätietojen merkityksellä ja muilla tiedonkeruumenetelmillä saatujen tietojen yhteiskäytön sopivuudella, hyödynnettävällä lisäinformaatiolla, jota ei tule sulkea pois prosessista. Tapahtumien ja tilanteiden tarkkailu sekä puheen ja toiminnan välinen vertailu tuottavat paljon lisätietoa ja sanatonta informaatiota, jota tutkimuksessa voidaan käyttää hyödyksi. Muilla tavoin kerättyjen tietojen lisäksi havainnointi lisää varmuutta johtopäätöksien tekemiseen.

Ulkopuolisen auditoijan ja havainnoijan etu on, ettei tutkija katso minkään tietyn ennako- asenteen tai tilanteen näkökulmasta analysoitavia asioita. Tutkimuksen objektiivisuus ei kärsi myöskään silloin siitä, että auditoija olisi sitoutunut emotionaalisesti auditoitavaan kohteeseen. Havainnointi sopii myös erityisen hyvin toteutettavaksi yhdessä kvalitatiivisen haastattelun kanssa samanaikaisesti. Havainnoin lajina on tähän tutkimukseen valittu ulkopuolisena havainnoijan vapaasti tilanteeseen muovautuvaa menetelmää, joka tukee kvalitatiivista tutkimustapaa. (Hirsjärvi ym.2009, 207 - 208.)

Auditoinnin aikana auditoija toteutti sekundäärisenä tiedonkeruumuotona havainnointia keräämällä ja laittamalla muistiin tietoja organisaation toiminnasta ja turvallisuuskulttuurista sekä toimintatapamenetelmistä. Havainnointia tehtiin erityisesti esimiesten ja organisaation käyttäytymisestä, valmiudesta ja asennoitumisesta turvallisuusasioihin. Havainnointia tehtiin kokonaisvaltaisesti koko auditointiprosessin ajan, kesästä syksyyn. Havainnoinnilla pyrittiin löytämään lisää sellaista tietoa, jota ei toteutetuissa kyselyissä tai haastatteluissa olisi saatu. Havaintotietoja kerättiin esimerkiksi käytyjen keskustelujen, pyyntöjen, kyselyjen ja niistä saatujen vastausten sekä tietojen että toteutumien perusteella analysoimalla ja vertailemalla toimintaa, kestoa ja itse sisältöä toisiinsa. Havainnointia tehtiin myös tapaamisten yhteydessä ja kaikesta paikan päällä tapahtuneista auditoijan tekemistä näkö- ja kuulohavainnoista.

5.2.5 Tietoaineiston analysointi

Kerätyn tietoaineiston analysointi, tulkitseminen ja johtopäätösten teko on tutkimuksen tärkein ydinasia, johon tähdätään tutkimuksen alusta lähtien. Vasta tietoaineiston analyysivaiheessa selkeytyvät tutkimuksen ongelmat ja kuinka ongelmat olisi alun alkaen pitänyt asettaa sekä minkälaisia vastauksia on saatu ongelmiin. Empiirisen tutkimuksen tietoaineistosta voidaan tehdä päätelmiä vasta, kun tietoja on ensin esikäsitelty. Esikäsitelyn vaiheita ovat tietoaineiston tarkistus, täydennys ja järjestäminen. Tiedon tarkistuksessa kiinnitetään huomiota virheellisyyteen ja puutteellisuuteen. Tietoja voidaan täydentää, kuten tässä tutkimuksessa dokumenttiaineistoa täydennetään haastatteluilla ja täsmennetyillä tarkistuskyselyillä. Tietoaineiston, kuten tässä tutkimuksessa käytetyn kirjallisen kyselyaineiston järjestäminen, on suuritoisin osuus koko tietoaineiston analysoinnissa. (Hirsjärvi ym.2009, 216 - 217.)

Tämän tutkimustyön tarkastelu tapahtui analysoimalla kohdeyritykseltä saatuja dokumentaatiota, kyselyistä saatujen vastauksia vertailemalla, haastatteleamalla yrityksen johtoa ja turvallisuudesta vastaavia, havainnoimalla ja seuraamalla käytäntöjä sekä toimintoja. Monipuolisesti ja useista eri lähteistä kerättyjä sekä saatuja tietoja verrattiin toisiinsa, jonka perusteella hahmotettiin yrityksen turvallisuuden nykytilanne ja -taso. Aineiston luotettavuutta ja validisuutta lisättiin edellä esitettyjen menetelmien triangulaatiolla ja päällekkäisyyksillä.

Tässä tutkimuksessa saatujen tietojen analysointi perustui aineiston luokitteluun, teemoitteluun ja tyypittelyyn, joiden mukaisesti pyrittiin vielä analysoimaan haastatteluvastausten sisältöä. Strukturoiduissa kyselyissä toteutettiin sekä laadullinen (kvalitatiivinen) eli selittävä osuus että määrällinen kyselytutkimuksen (kvantitatiivinen) osuus. Turvallisuudesta laaditut kysymyssarjat muodostivat tutkimuksen yhden tietolähteen, jonka perusteella tehtiin auditointitulosten arviointia ja täydennettiin analysointituloksia varten tarvittavilla lisätarkennuksilla. Tarkennukset saatiin dokumentaatioihin perehtymällä ja johdon antamien haastatteluvastauksien yhteisvaikutuksesta. Havainnoinnin osuutta pidetään analysoinnissa vain triangulaatiota vahvistavana lisätietona. (Hirsjärvi ym.2009, 219 - 220.)

6 Auditointitulokset Katakryn mukaan

Tämä luku on rakennettu siten, että ensin esitellään yleiskuvan muodostamiseksi tuloksena saadut pääkohdat ja toiseksi yleiskuvaus nykytilasta ja tasosta sekä päähuomiot tilanteesta, joka muodostui auditoinnin aikana. Tämän raportin lopussa esitetään liitteinä auditoinnista tehdyt poikkeama-arvioinnit kriteeristön kysymyksiin, Katakryn osa-alue järjestyksen mukaisesti. Liitteissä ensin kahdella sivulla näytetään turvallisuuskyselystä tehdyt koosteet ja sen jälkeen Katakryn kriteerikysymysten mukaisessa järjestyksessä arvioidut poikkeamatulokset. Huomioitava on, että tuloksiin on päädytty poikkeama-arviointien mukaan, jotka on tehty Ka-

takrin näkökulmasta ja kriteeristön vaatimuksiin perustuvista vertailuista. Arvioinnit on tehty periaatteella ”esitä dokumentti tai selitä mitä on tehty ja miten”, olettamuksia ei ole otettu mukaan, jotta ulkopuolisen arvioijan olisi ollut helpompi arvioida tuloksia objektiivisesti.

Auditoinnissa kartoitettiin yrityksen X kokonaisturvallisuuden nykytilanne. Kartoitus on suoritettu käyttämällä hyväksi Katakri II:n ja Katakri 2015 turvallisuuskriteeristössä esitettyjä kysymyksiä viitearvoina ja apuvälineinä nykytilanteen todentamiseen. Kohdeyrityksen nykytilaa verrattiin Katakri II:ssa esitettyyn, elinkeinoelämän suositusten mukaiseen tavoitetasoon. Katakri 2015:a ei ole EK:n suojaustasovaatimustasoa esitetty hallinnollisen turvallisuuden osa-alueissa vaan niissä esitetään vain minimivaatimustaso, joka tulisi täyttää. Auditointi rajattiin käsittämään Katakri II:n hallinnollisen turvallisuuden ja turvallisuusjohtamisen osa-alueet (A100 - A900), 63 kysymysaluetta sekä juuri ilmestyneen Katakri 2015 osalta, hallinnollisen turvallisuuden turvallisuusjohtamisen osa-alueita koskevat (T1 - T7) seitsemän ensimmäistä kohtaa. Katakriin kysymysosa-alueiden yhteenlaskettu määrä oli 70, joista jokaisesta esitettiin muokattuja pää- ja lisäkysymyksiä haastateltaville sekä kyselyyn osallistujille.

Auditoinnista saatujen tietojen käsittelyssä käytettiin kolmiportaista poikkeama jaottelua kehittämiskohteiden analysoinnin ja arvioinnin helpottamiseksi. Kohdeyrityksen nykytilaa verrattiin Katakriin esitettyyn, elinkeinoelämän suositusten mukaiseen tavoitetasoon (EK:n tasoo). Arviointiasteikkona käytettiin seuraavaa poikkeama luokittelua:

1. **Vihr** Ei poikkeamaa (kriteerin vaatimus täyttyy)
2. **Kelt** Lievä poikkeama (vaatimus ei täyty, mutta poikkeama ei ole vakava)
3. **Pun** Vakava poikkeama (kriteerin vaatimus ei täyty ja poikkeama on vakava)

Kyselyt osoitettiin kohdeorganisaatiossa yhteensä 57 henkilölle, joita olivat työnjohdollisissa ja esimiestehtävissä toimivat henkilöt sekä ylin johto. Vastausprosentti oli 86 %:n, vastaajamäärän ollessa 49 kappaletta, joista kahdeksan ei vastannut kyselyyn. Kohdeorganisaation esimiehistöille osoitettiin 101 kysymyksen sarja ja ylimmälle johdolle edellä mainittujen lisäksi vielä 40 lisäkysymystä. Kyselyjen tarkoituksena oli saada aikaan numeerinen vertailutilanne, jota laajennettiin ja täydennettiin auditoinnissa muilla keinoin saaduilla tiedoilla.

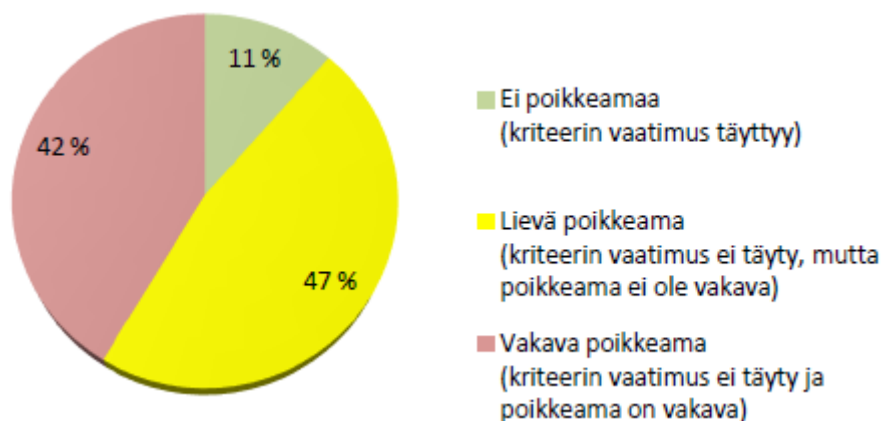
Kyselyn numeraalista vertailua perustellaan sillä, että kaikki kysytyt asiat ovat silloin, samalla arvoasteikolla toteutettuna vertailutettu suhteessa toisiinsa. Jos kysytty asia ei ollut edes tuttu tai sitä ei edes osattu mitenkään kommentoida tai arvioida, voitiin tuloksen perusteella vetää yhtenä johtopäätöksenä, ettei kohdeorganisaatiossa sitä silloin ole toteutettu ei ainakaan kunnolla, eikä kysytty vaatimus tai asia kriteerin mukaan silloin myöskään täyty. Kyselyllä saatiin tietoa turvallisuusasioiden tietämystasosta ja suhteesta toisiinsa. Ensisijainen tavoite oli kuitenkin käyttää tuloksia myös itse poikkeama-arviointien tukena, joka toteutui vain osittain, sillä itse kyselyn aikana ilmeni osassa kysymyksiä tulkinnallisia eroavaisuuksia. Audi-

toija ei ollut onnistunut muotoilemaan kaikkia kysymyksiä riittävän ymmärrettäviksi tai selkeiksi ja osassa kysymyksiä esitettiin turvallisuustermejä, jotka eivät olleet tuttuja. Kyselyn tulokset on esitetty tarkemmin tämän työn lopussa liitteet osiossa johon on sijoitettu myös Katakriin mukaiset poikkeama-arviot osa-alueiden mukaisessa järjestyksessä.

6.1 Auditoinnista saadut arviointitulokset

Katakri II:n ja Katakri 2015 hallinnollisen turvallisuuden ja turvallisuusjohtamisen osa-alueista arvioitiin yhteensä 70 pääkriteeristön vaatimusta ja pääkysymyskohtaa. Auditoinnista saatu kokonaistulos on esitetty alla olevassa piirakkakuviossa (kuvio 6). Auditoointituloksen mukaan 8 kysymystä 70:stä (11 %) oli kriteeristön vaatimusten mukaisesti arvioituna täytetty, joka näkyy kuviossa esitettynä vihreänä ”Ei poikkeamaa” osuutena.

Piirakkakuviossa (kuvio 6) on, kriteeristössä esitettyihin pääkysymyksiin, esitetty keltaisella lievien ja punaisella vakavien poikkeamien arvioidut osuudet. Auditoointituloksen mukaan 33 kysymystä 70:stä (47 %) jäi kriteeristön vaatimusten mukaisesti arvioituna täyttämättä, mutta poikkeamien arvioitiin olevan joko osittain täytetty tai lieviä. Auditoointituloksen mukaan 29 kysymystä 70:stä (42 %) jäi kriteeristön vaatimusten mukaisesti arvioituna kokonaan täyttämättä ja poikkeamat arvioitiin olevan joko vakavia tai hyvin vakavia turvallisuuspuutteita.



Kuvio 6: Katakriin mukaisen poikkeama-arvioinnin kokonaistulos

Taulukossa 1 on esitetty tulokset tarkemmin eriteltynä, Katakriin hallinnollisen turvallisuuden osa-alueiden A ja T mukaisesti jaoteltuna (taulukko 1). Esitysjärjestys on poikkeamien suhteellisen lukumäärän mukaisessa järjestyksessä, jossa on esitetty ensimmäisenä ja ylimpänä vakavimmin ja alimmaisena lievimmän puutteellisuuksia omaava osa-alue. Ongelmallisista tai puutteellisista turvallisuuden osa-alueista, jotka jäävät heikoin täyttämättä, on Katakri 2015 hallinnollisen turvallisuuden ja turvallisuusjohtamisen osa-alue (T 01 - T 07), sillä 7 pääkysymysalueesta vain kaksi (28,6 %) oli arvioituna lieviä poikkeamia ja loput (71,4 %) vakavia. Par-

haiten vaatimukset täyttyneet osa-alue käsitti turvallisuusdokumentaatioita ja niiden hallintaa, jossa puolet (50 %) täytti kriteeristön vaatimukset ja loput olivat lieviä poikkeamia. Huomattavaa kokonaisarvioinnissa on, että mitään pääosa-alueita, valittujen EK:n suojaustasojen ja perustason mukaisesti, ei kokonaan läpäisty tai kriteeristössä esitettyä vaatimusta täytetty.

Taulukosta 1 näkee, että auditoinnista tehdyt poikkeama-arviot jakautuivat tasaisen sekaisesti koko turvallisuuskentän eri osa-alueille. Tämä johtuu siitä, että organisaatio on keskittynyt erittäin hyvin työturvallisuusasioihin ja siihen liitettyihin henkilö-, tila- ja paloturvallisuusasioiden hallitsemiseen. Kokonaisturvallisuus on kuitenkin jäänyt vähemmälle huomiolle, jota myös auditoinnista saadut haastattelut ja kirjalliset kyselytulokset tukevat. Saatu kokonaistulos poikkeama-arvioineen antaa kuitenkin hyvän yleiskuvan turvallisuuden nykytilan tasosta yrityksessä X, jota myös kvantitatiivisen kyselyn tulos osaltaan tukee ja vahvistaa.

Taulukko 1: Poikkeama-arvioinnin tulokset turvallisuuden eri osa-alueiden pääkysymysten mukaisesti eriteltyinä jotka on esitetty puutteellisimmasta osa-alueesta lievimpään.

OSA-ALUE: A Hallinnollinen turvallisuus

KATAKRI II:n mukaan (A100 - A900) ja III:n mukaan (T 01 - T 07)

Jnro	YHT	Vihr	Kelt	Pun	Kysymysten määrä:						
					kpl	kpl	kpl	kpl			
10	T1-7	KATAKRI III mukaan Hallinnollinen turvallisuus - Turvallisuusjohtaminen	7	0	2	5	0,00 %	28,57 %	71,43 %	2,71	
9	A300	Turvallisuuden tavoitteiden määrittely	6	0	2	4	0,00 %	33,33 %	66,67 %	2,67	
8	A600	Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet	8	0	3	5	0,00 %	37,50 %	62,50 %	2,63	
7	A900	Raportointi ja johdon katselmukset	5	1	1	3	20,00 %	20,00 %	60,00 %	2,40	
6	A400	Riskien tunnistus, arviointi ja kontrollit	12	1	6	5	8,33 %	50,00 %	41,67 %	2,33	
5	A500	Turvallisuusorganisaatio ja vastuut	7	0	5	2	0,00 %	71,43 %	28,57 %	2,29	
4	A200	Turvallisuuden vuotuinen toimintaohjelma	4	0	3	1	0,00 %	75,00 %	25,00 %	2,25	
3	A100	Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt	9	1	5	3	11,11 %	55,56 %	33,33 %	2,22	
2	A800	Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen	8	3	4	1	37,50 %	50,00 %	12,50 %	1,75	
1	A700	Turvallisuusdokumentaatio ja sen hallinta	4	2	2	0	50,00 %	50,00 %	0,00 %	1,50	
					YHT	Vihr	Kelt	Pun			
					70	8	33	29	11,43 %	47,14 %	41,43 %

Arviointiasteikkona käytetään seuraavaa poikkeama luokittelua:

YHT	Osa-alueesta esitettyjen kysymysten määrä (kpl)
Vihr	Ei poikkeamaa (kriteerin vaatimus täyttyy)
Kelt	Lievä poikkeama (kriteerin vaatimus ei täyty, mutta poikkeama ei ole vakava)
Pun	Vakava poikkeama (kriteerin vaatimus ei täyty ja poikkeama on vakava)

KA = Maksimi 3 ja minimi 1
Mitä pienempi arvo on, sen parempi.

Jnro = Järjestysnumero
Mitä pienempi numero sitä paremmin on asiat

Kehittämisenäkökulmasta saatu epätasaisuustieto ei johda riittävän tehokkaaseen turvallisuusasioiden parantamiseen tähtäävään ehdotuslistaan, jossa turvallisuuden osa-alueet olisi listattu puutteellisuusjärjestyksessä. Tästä auditointia teki sen johtopäätöksen, että kehittämissuhteeseen paremmin pääsemiseksi, oli etsittävä tulosten mukaan toinen hyödyntämisen näkökulma. Tästä syystä, raportissa kehitysehdotukset ovat rakennettu ja esitetty luvussa 7, auditoinnista saadun yleiskuvan ja ”tehtävien vastuunjakoon” perustuvalla periaatteella.

6.2 Turvallisuuden nykytilan ja tason arviointi

Suoritetun auditoinnin perusteella yrityksen X turvallisuuden nykytilaa voidaan pitää tyydyttävänä. Katakryn poikkeamatulokset eivät valitettavasti kerro, että turvallisuusasioita ja -toimia on tehty myös oikein, oikean suuntaisesti ja jopa riittävällä tasolla. Auditoinnista saatujen tulosten perusteella voidaan todeta, että organisaation työ-, henkilö-, tila- ja paloturvallisuusasioissa on tehty huomattavia parannuksia muutaman vuoden sisällä. Parantunut turvallisuuskehitys näkyy myös tapaturmatilastoissa. Aihioita ja toimintoja on monissa asioissa aloitettu oikein ja niitä jatkamalla saadaan edelleen puutteita korjattua ja parannuksia tehtyä. Monissa tapauksissa yksittäisen, kriteeristön vaatimuksessa esitetyn, asiakohdan puuttuminen ratkaisi lopullisen poikkeamatuloksen lieväksi poikkeamaksi. Kehitystyötä jatkamalla voidaan, Katakryn kriteeristönkin mukaan, arviointitulosta saada muutettua nopeasti paremmaksi sekä suositusten mukaisia lieviä poikkemavaatimuksia täytettyä. Koska tämän auditoinnin tarkoituksena oli keskittyä löytämään ja todentamaan kohdeorganisaation hallinnollisen turvallisuuden epäkohtia, heikkouksia ja puutteita, ei sen takia ole hyvin hoidettuja asioita ja onnistumisia tässä raportissa erityisen laajasti esitelty tai käsitelty.

6.2.1 Turvallisuustoiminnan toteuttamisen ongelma

Kerättyjen auditointitietojen valossa voidaan erityisesti huomioida, että turvallisuusasioita tehdään epätasaisesti eri hierarkiatasojen välillä ja saman hierarkiatason toimijoiden kesken. Auditoinnin eri vaiheissa nähtiin, kuultiin ja havaittiin, että turvallisuusasioita pidetään tärkeinä ja tiedostetaan vastuut. Resurssien rajallisuuden vuoksi seuranta, valvonta ja varmistamistoimet sekä tärkeät tiedottamiset jäävät kuitenkin tekemättä, koska aika ei enää riitä lisätehtävien hoitamiseen. Toiminnan ja tekemisen taso ei pysy siten tasalaatuisena tai esimerkiksi tiedon kulku ei saavuta kaikkia tahoja, kun varmistamistoimenpiteet jäävät tekemättä.

Samalla auditoinnin tuloksena havaittiin, että epätasaiseen turvallisuuden toteutumiseen ja niiden ymmärtämiseen liittyy myös kielellisiä ja kulttuurillisia ongelmia. Nämä ongelmat osataan syntyvät työnjohdollisten toimijoiden käytännön toiminnan toteutuksessa havaituista eroista. Toimintatapaeroja syntyy myös, kun itse toteuttaja ja kohde eivät kommunikoinnissaan kohtaa. Suurimmat epätasaisuudet todettiin perehdytyksessä ja koulutuksessa sekä erityisesti turvallisuustoiminnan seurannassa, valvonnassa ja luottamuksellisen tiedonkäsittelyssä. Kaikkiin mainittuihin ongelmiin on todettavissa selkeä resurssiongelma, joka on sen verran merkityksellinen, että nykyisessä muodossa se ei takaa esimiehistöille roolinsa mukaista realistista onnistumisen mahdollisuutta kokonaisturvallisuuden ylläpidossa ja kehittämisessä.

Mielenkiintoisena yksityiskohtana on todettava, että yrityksen X turvallisuusjohtamisesta on tehty erittäin hyvä powerpointesitys, jossa yleisen turvallisuuden kokonaiskuva on hyvin tuotu

esille yrityksen X näkökulmasta. Kyseinen esitys on siksikin hyvä, että siihen on kiteytetty kaikki kokonaisturvallisuudesta huomioitavat seikat lisättynä vastuunjaolla, ”meidän riskeillä” ja turvallisuusjohtamiseen liittyvillä asioilla. Tämä on kuitenkin, auditointitulosten perusteella, jäänyt jostain syystä kunnolla toteuttamatta tai sitten turvallisuusjohtamisen mallia ei ole vielä saatu ajettua läpi eri hierarkiatasoille. Osasyynä voi olla myös, että sitä ei ole jatkaloistettu riittävästi tarjoilukelpoiseen muotoon tai integroitu osaksi esimiehistön turvallisuuden koulutuspakettia. Laadittu esitys, johon johto näkyvästi sitoutuu, on tuotava kaikille turvallisuudesta vastaaville esimiehille koulutuksiin mukaan. Esitys tuo monia kokonaiskuvaavien selkeyttäviä asioita esiin, kuten rooleihin, tehtäviin ja vastuihin liittyvää tietoa sekä kaivattua turvallisuuskulttuurillista pohjaa, jolla myös parannetaan yrityksen kokonaisturvallisuutta.

6.2.2 Turvallisuudesta vastaavien työnkuvat, vastuut ja organisointi

Auditoinnissa ilmenneiden tietojen mukaan yrityksessä X turvallisuudesta vastaavien henkilöiden työnkuvia ei ole dokumentoitu yrityksen järjestelmiin eikä kirjattu työsopimuksiin. Turvallisuusjohtamisen tehtäviä, vastuita, rooleja ja käytettävissä olevia resursseja ei ole kirjattu auki, eikä niitä ole tarkkaan yksilöity. Normaalityilanteiden työnjohtotehtävien hoidossa tämä ei muodosta suurta haittaa, mutta epäkohta realisoituu ongelma- tai poikkeustilanteiden aktivoituessa tapahtuman suuruuden mukaan. Tilanteissa, joissa pitää keskittyä ongelman tai poikkeustilanteen nopeaan ratkaisemiseen vastaavalla esimiehellä ei ole aikaa organisoida, järjestäytyä ja asemoida omaa rooliaan ja valtuuksiaan tapahtumien keskipisteessä vaan tilanteen nopea normalisoiminen on aina ensimmäisenä prioriteettina. Samalla voidaan esittää väittävä, ettei turvallisuudesta vastaaville henkilöille ole kanavoitu riittävästi aikaa seurata, valvoa, vastata, vaikuttaa ja kehittää turvallisuustoimintaa omassa roolissaan.

Johtopäätöksenä oli todettu, että yrityksessä toimii vain työturvallisuuden mukainen työ-, henkilö-, tila ja paloturvallisuuteen keskittynyt työsuojelutoimikunta ja organisaatio, joka ei kuitenkaan toimi ja ota huomioon yrityksen kokonaisturvallisuuteen liittyvien osa-alueiden johtamista, hallintaa ja kehittämistä. Työsuojeluorganisaatio ei myöskään varmista, auditointitulosten ja tietojen mukaan, että jokainen työntekijä ja esimies todella tietäisi, miten toimia oikein poikkeamatilanteissa ja kuka vastaa ja mistä saa apua tai tukea. Vaikka perehdytyslomakkeessa edellytetään näiden asioiden läpikäyntiä, auditoinnin mukaan on suuri joukko vielä niitä, jotka eivät todella tiedä, miten toimia tai kenelle ilmoittaa asioita.

Työtehtäväkuvausten ja vastuiden puuttuminen prosessikuvauksista, järjestelmistä tai kohdekansioista sekä turvallisuusorganisaatioon kuulumisesta on suuri puute, kun huomioidaan yrityksen liiketoiminnan koko maata kattava laajuus sekä henkilöstön ja palvelukohteiden lukumäärä. Turvallisuusvastuiden, -valtuuksien ja -tehtävien näkymättömyys työnkuviissa on myös Katakriin mukaan epäkohta. Kokonaisturvallisuuden toimintaedellytykset luodaan selkeillä re-

surssoinneilla ja organisoinneilla. Jokaisen turvallisuudesta vastaavan henkilön oman oikeusturvan kannalta on tärkeää tietää, mitä vastuuasioita tehtäviin kuuluu ja mitä vaaditaan normaalista poikkeavissa kriisitilanteissa. Dokumentoidut työnkuvaukset myös selkeyttävät vastuukysymyksiä ja tehostavat esimiesten toimintaa, työn priorisointia ja ajankäyttöä.

6.2.3 Turvallisuusorganisaatio ja tilannekuva

Turvallisuusorganisaation puuttuminen on myös Katakryn mukaan ongelma. Turvallisuusorganisaation tulisi vastata, ylläpitää, seurata ja jatkuvasti kehittää yrityksen kokonaisturvallisuutta. Turvallisuusorganisaatio on järjestäytynyt elin, joka koostuu yleensä yrityksen johtoryhmään kuuluvista ”oman toimen ohella” vastuutetuista ylemmistä toimihenkilöistä, joilla on nimetty omat vastuualueensa turvallisuuden kehittämisessä. Samalla kun johtoryhmän koontuu, työlistalla on muiden käsiteltävien asioiden lisäksi vakiona myös turvallisuusasioita. Tämän toiminnan toteutuminen edellyttää, että tehtävät ja vastuualueet ovat kirjattuja rooleineen ja valtuuksineen, organisaatio julkaistu kaikille ja henkilöt sitoutuneita tehtäviinsä. Turvallisuusorganisaatiolla on oltava myös oma toimintatapaohjeistus sekä tietyn tason valmiusvelvoite kokoontua pikakokouksiin vakavissa poikkeamatilanteissa.

Yrityksen johdon tulee olla hyvin perillä turvallisuustilanteesta, jota ylläpidetään kokonaisturvallisuuden tilannekuvalla. Kokonaisturvallisuuden mukaista tilannekuvaa ei tuoteta, jos ei ole selkeää organisoitua tiedonkulkuun, päätöksentekoon ja raportointiin sovittua toimintatapamenettelyä, joka vielä varmistaa, että tieto kulkee varmasti molempiin suuntiin ja perille asti. Auditoinnissa esitetty toimintatapamenettely, jossa työsuojelupäällikölle lähetetään poikkeamatiedot tai turvallisuusilmoitus, toimii niin kauan kun varmistetaan, että kaikki tiedot myös kirjataan, lähetetään oikeaan osoitteeseen ja ne tulevat perille. Toimintaa kehitettäessä ja järjestettäessä on huomioitava hyväksyttävissä oleva aikaviive vastatoimien aloittamiselle siitä, kun tilannekuva poikkeavan tilanteen johdosta muuttuu. Käytännön toimintaa tulisi myös testata ja mittaamalla varmistaa turvallisuuspoikkeamatiedon lähettämiseen, käsittelyyn, päätöksentekoon ja itse toteutettavaan vastatoimintaan kulunut yhteisaika.

6.2.4 Riskienhallinta

Arvioinnissa kiinnitettiin huomiota myös yrityksen kokonaisturvallisuuden riskien hallintaan. Asiakaskohteisiin riskienarviointia tehdään aina kohteen alussa kohde-esimiehen toimesta, mutta ongelmana on arviointien epäsäännöllinen päivittäminen. Nykyinen käytäntö on tarpeellinen ja hyvä työturvallisuuden, kohteen yleisen arvioinnin ja liiketoiminnan lähtökohdista, mutta se ei kata kokonaisvaltaisesti yrityksen riskejä ja uhkia. Auditointikriteeristö lähtee kuitenkin siitä, että organisaation riskejä tulee hallita kokonaisvaltaisesti, säännöllisesti ja prosessimaisesti sekä riskienarviointi tulee olla yrityksen turvallisuustyön lähtökohta ja perus-

te. Riskienhallinnasta puuttuu myös järjestelmällisyys, sillä riskien kartoittamiseen ja analysointiin tulee käyttää vakiintunutta, avointa ja ymmärrettävää menetelmää. Riskienarviointia tulee toteuttaa myös eri menetelmin sen mukaan, onko kohteena normaali toiminta, erityistilanne vai hätätapaukset ja tässä tapauksessa asiakaskohde vai konttori. Riskienarvioinnissa tulee huomioida myös, miten tuloksia käsitellään, analysoidaan, luokitellaan, dokumentoidaan, viestitetään ja vaikuttavuutta arvioidaan päätettäessä suojaustoimista.

6.2.5 Turvallisuudelle asetetut tavoitteet

Auditointitulosten mukaan yrityksen johtoryhmä asettaa hyviä tavoitteita, mutta toteutusta varten ei valita menetelmiä, lukita aikatauluja, nimetä vastuuhenkilöitä eikä esitetä tavoitteille vaatimusmäärittelyä tai aseteta seurantamittareita. Turvallisuuspolitiikassa on esitetty, että käytössä olisi johdon tuloskortti, mutta sen käytöstä ei ole saatu luotettavaa tietoa. Tuloskortin käyttäminen kaikkine ominaisuuksineen voisi korjata edellä mainitut turvallisuudelle asetettujen tavoitteiden hallinnasta löydetyt puutteet. Työsuojelutoimikunnan toiminnassa ennaltaehkäisykeinojen tavoitteenasettelu ja toteutustoimenpiteiden johtaminen sekä seuranta ovat hallinnassa. Heikkoutena on kuitenkin, että työsuojelutoimikunnan toimintakentän vaikuttamislaajuus ei kata koko yrityksen kokonaisturvallisuuden jatkuvaa kehittämistä ja parantamista, eikä työsuojelu ole oikea taho, jossa kokonaisturvallisuuden asioita käsitellään.

6.2.6 Tietohallinto

Auditoinnissa muodostui suurimmaksi kysymykseksi tietohallinnossa toteutetut järjestelyt. Ilmeni, että tietotekniset asiat ovat ulkoistettu yritykselle, jonka turvallisuutta ei ole yrityksen toimeksiannon yhteydessä auditoitu eikä turvallisuuden näkökulmasta riskejä ja uhkia kartoitettu. Auditoinnin aikana selkeytyi kuva tietohallinnon tärkeydestä koko maata kattavan liiketoimintaverkon ja järjestelmien ylläpitämisessä. Eli liiketoiminta on riippuvainen tietoliikenteen ja ICT -laitteiden toimivuudesta. Tietohallinto on myös osoittautunut yhdeksi yrityksen tärkeimmistä suojattavista kohteista, jonka mukaan tulee jo kansallisen mittapuun ja globaalin kyberturvallisuuden varmistamisen näkökulmasta tehdä suurin toiminnan jatkuvuuteen tähtääviä ja varmistavia päätöksiä sekä suunnitelmia, jotta liiketoiminta ylipäätensä voi jatkaa häiriötöntä toimintaansa poikkeustilanteistakin huolimatta sekä tietoturvaohjeita vältellen.

Auditoinnin aikana ei löytynyt mitään dokumentoitua tietoa, miten esimerkiksi yrityksen käyttöoikeuksia hallitaan ja pääsynhallintaa toteutetaan eri järjestelmiin eikä, miten varmistetaan ja valvotaan, ettei vaarallisia työyhdistelmiä synny. Käyttöoikeuksien myöntämisessä on toimintatapana käytössä olevien järjestelmien pääkäyttäjien hyväksymismenettely pyynnöstä, jota käsitellään esimerkiksi sen mukaan, mikä on työsuhteen status. Statuksensa mukaan toimihenkilö saa pääsyoikeuksia enemmän kuin työntekijä. Auditoinnissa ei saatu tarkkaa sel-

vyyttä, kuinka automaattisesti oikeuksia jaetaan eikä, miten laajaa tai kattavaa oikeutta jaetaan ja onko järjestelmien välille laadittu tehtävän mukaisia rajoitteita.

Auditointitulosten mukaan yrityksessä ei ole järjestelty tietohallintoon liittyviä asioita eikä kokonaisvastuuta ole asetettu, yksilöity tai kuvattu kenellekään. On vain toimijoita, jotka suorittavat tuki- ja ylläpitotoimia. Tämä on huolestuttavaa, koska vastuuta ei voi ulkoistaa, vaikka toimintojen ylläpito olisikin ulkoistettu. Ulkoistamisesta huolimatta yrityksellä tulee olla aina myös riittävä tietotekninen ja tietoturva-asioiden asiantuntemus sekä taito alalta.

Yrityksen dokumentaatioissa ei ollut myöskään tietoa tehdyistä, tietohallinnon alueeseen kuuluvista, toimintasuunnitelmista, seuranta- ja kehitysprojekteista eikä omasta erillisistä muutoksenhallintamenettelyistä. Auditointitulosten mukaan ja yrityksen dokumentaatioista ei myöskään löytynyt merkkejä toteutetuista suunnitelmista, miten tietoturva hallinnollisesti, teknisesti ja fyysisesti hoidetaan. Tietoturvallisuuskulmaa ei, auditoijan oman tietoturvakokemuksen mukaan, ole otettu tietoturvaohjeistuksissa riittävästi huomioon ja tietoturva-poikkeamien käsittelystä ei ole laadittu toimivaa erillistä toimintatapamenettelyä.

Yrityksellä ei ole myöskään julkaistu tietoturvapoliittikkaa eikä määriteltyä eikä toteutettua tietoturvasuunnitelmaa. Ulkoistetun palveluntuottajan toiminnan hallinnasta ja salassapitosopimuksista tai palvelutasolupauksista ei ole yhtään mainintaa tai dokumentaatiota. Tietoteknisistä toimintojen suojaus-, varmistus-, jatkuvuudenhallinnan ja palautustoimista ei ole tehty mitään suunnitelmia eikä vaadittavista menettelytavoista eikä toiminnoista mitään ohjeita.

7 Katakriin mukaan tehdyt kehittämissuositukset

Tässä luvussa esitetään auditoinnin tuloksista, analyseista ja arvioinneista tehdyt johtopäätökset. Luvussa käsitellään ensin yleistilanteen mukaista toimintatapaehdotusta sekä selitystä alalukujen järjestykselle ja esityslogiikalle. Tämän jälkeen paneudutaan tarkemmin alaluvuissa esitettyihin, pääaiheiden mukaisiin kehittämissuosituksiin. Alaluvut on rakennettu vastuujonon mukaan siten, että ne muodostavat omat puutelistat, joita tässä auditoinnissa saatujen tietojen ja havaintojen perusteella pidettiin merkityksellisinä tai muutoin erityisen tärkeinä. Esitysjärjestys ei noudata Katakriin kriteeristön osa-alueiden mukaista järjestystä vaan kokonaisturvallisuuden hallinnan ja kehitystehtävien mukaan tehtyjä aihekokonaisuuksia.

Auditointitulosten esitysjärjestykseen on vaikuttanut yrityksen kokonaistarpeet ja hyötynäkökohdat. Ensimmäisenä esitetään kokonaispainoarvoltaan ja vaikuttavuudeltaan puutteellisimmaksi osoittautuneita turvallisuuden osa-alueita tai kehittämiskohteita. Tällä järjestelyllä on pyritty myös siihen, että jokaisella erikoisosa-alueella toimivaa vastuuhenkilöä kuormitettaisiin korjaustoimissa tasaisemmin. Samalla pyritään huomioimaan, että kehittämiskohteet voi-

taisiin aloittaa melkein samanaikaisesti eri osa-alueilla, jolloin parannus ja kehittämistyö olisi kokonaisvaltaisempaa ja tehokkaampaa suorittaa lyhyemmässä ajassa. Tulkinta lähtee oletuksesta, että kehittämiskohteissa ei ole sellaista estettä, mitä ei pystyisi valmistelemaan ja kehittämään samanaikaisesti. Jaottelussa on myös pyritty, arvioidun selvityksen ja auditoijan oletuksen mukaisesti, joko jakamaan kehitystoimintoja yrityksen vastuujonon mukaisesti tai sen mukaan, miten turvallisuusasioiden hoitamisen perusteella olisi optimaalisinta.

Yrityksen X toimintatapoihin, päätöksentekoprosesseihin tai valmistelu- ja hyväksymismenetelytapoihin puuttumatta, esitetyllä jaottelulla on ollut pyrkimys tuoda esiin, ehdotettujen kehitystoimenpiteiden ensimmäinen oletettu käsittelytaho, jonka käsittelyn mukaan prosessi sitten jatkaa etenemistään. Samalla halutaan korostaa, että kaikki tässä luvussa esitetyt kehitysehdotukset perustuvat Katakriin mukaan suoritetun auditoinnin mukaisiin priorisoituihin arviointituloksiin ja poikkeamiin, joiden on katsottu olevan vakavia tai vähintäänkin lieviä. Tulosten arvioimisen sijaan on tärkeämpää, mitä päätöksiä ja ratkaisuja kehittämistoimenpiteistä tullaan tästä eteenpäin tekemään kuin se miltä tulokset nyt näyttävät.

Esimerkkinä esitetään ylimmän johdon kategoriaan sijoitetut tehtävät, jotka oletetaan kuuluvan päätöksenalaisiin toimiin. Pyrkimyksenä on ollut kerätä yhteen kaikki ne ensivaiheessa käsiteltävät päätösaasiat, joiden mukaan on hyvä edetä valmisteluprosessien aloittamiseksi. Kaikkia asioita tulee ensin tilanteen mukaan harkita, koska on myös mahdollista, että jokin asia tai osa-alue ei ole vielä ajankohtainen tai se vain halutaan siirtää perustellusti tulevaisuuteen odottamaan suurempaa tarvetta tai sopivampaa ajankohtaa. Kaikkia asioita ei ole voinut laittaa myöskään kronologiseen toteutusjärjestykseen, sillä auditoinnissa ei tarkasteltu kohdeorganisaation päätöksentekoprosesseja niin tarkasti, että auditoija voisi esittää suoraan toimintatapojen mukaisesti ehdotuksia siinä järjestyksessä, miten asiat etenevät valmistelun tai eri vaiheiden kautta päätettäväksi.

Seuraavissa alaluvuissa on esitetty joukko kehittämisehdotuksiin liittyviä tarkistavia kysymyksiä, joihin toivotaan saavan perusteltuja vastauksia. Kysymykset sisältävät aihealueen, asian, tavoitteen tai toiminnan kohteeksi asetetun tilanteen, jonka mukaan toivotaan asioita tarkasteltavan tai asian suhteen heräävän yrityskohtaista turvallisuuteen liittyvää parantamiseen tähtäävää keskustelua. Peruseriaate kehitysehdotusten käsittelylle on, että ehdotusten mukaisesti kysymyksiin ei tule suoraan vastata ”kyllä” vaan kysymyksen mukaista tilanteen toteutumista tulee ensin tutkia. Jos kysymykseen vastaa suoraan myöntävästi, tilanne voi silloin johtaa uskomukseen, että asian suhteen kaikki on hyväksyttävällä tasolla. Tällöin tyydytään vallitsevaan tilanteeseen ja toiminnan taso säilyy ennallaan eikä mikään muutu, parane tai kehity. Näin voidaan menetellä, koska kohdeorganisaatiolla ei ole pakottavia velvoitteita toteuttaa vaadittuja kriteereitä tai tavoitetasoa. Tehtyjen päätösten tulee nojautua perustelliseen harkintaan ja hallittuun riskinottoon. Kehittämisehdotuksen tavoite on saavutettu sil-

loin, kun kysytty asia on tutkittu ja sen hyväksi tehty joitain ratkaisuja, muutoksia tai lisäyksiä ja näiden parantamistoimenpiteiden jälkeen voidaan kysymykseen vastata myöntävästi.

7.1 Turvallisuuden organisointi ja vuosikello

Turvallisuus ei ole mikään erillisesti liitettävissä oleva osa tai tukitoiminto vaan se on osana kaikkea yrityksen liiketoimintaa ja johtamistoimintaa eli tärkeä osa jo toimivaa kokonaisuutta. Turvallisuus tulee huomioida yrityksen strategiassa ja palveluissa sekä myytävässä tuotteessa, jotta itse palvelun tuottaminen tapahtuu turvallisesti ja itse tuote on turvallinen. Jos yrityksen yhdeksi päätavoitteeksi ei ole asetettu turvallisuutta, se ei toteudu myöskään palvelutapahtumassa. Turvallisuuden huomioimatta jättäminen tai sivuuttaminen voidaan myös tulkita asiakkaiden tai työntekijöiden puolelta siten, ettei turvallisuutta pidetä tärkeänä.

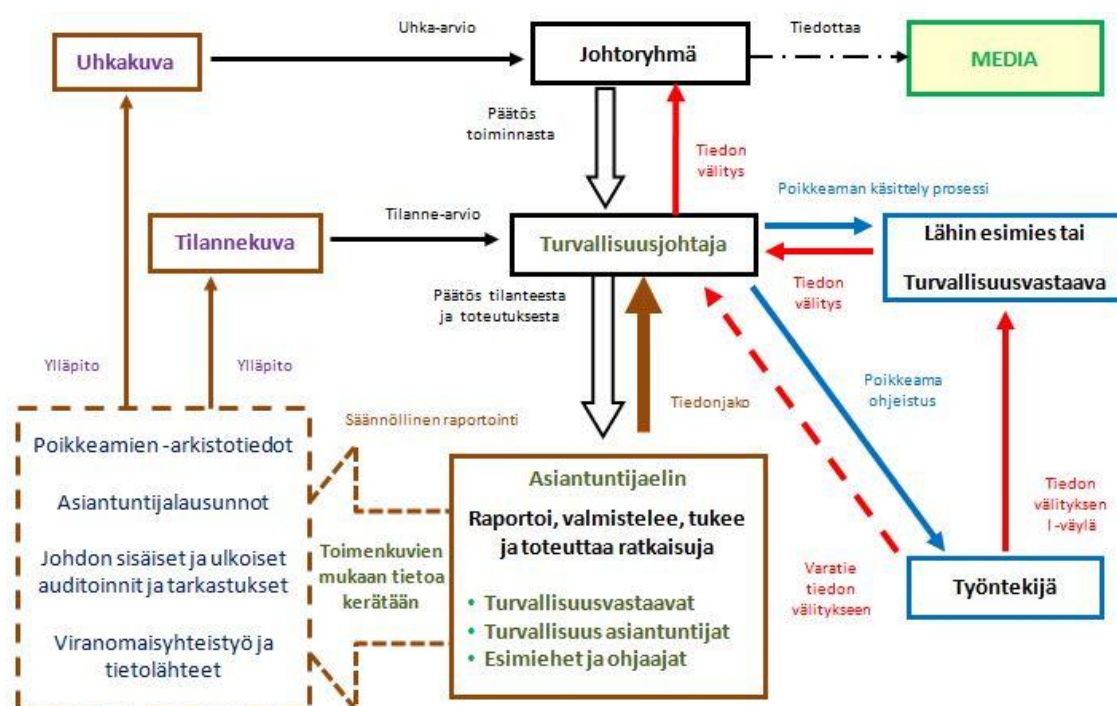
Näkyvin merkki vakavasta suhtautumisesta ja tärkeänä pitämisestä on, kun turvallisuusasiat on järjestetty mahdollisimman selkeästi, avoimesti ja organisoidusti. Kun yrityksellä on muodostettu virallinen turvallisuusorganisaatio, joka on myös tiedotettu yrityksen kaikille työntekijöille, kuvastaa se myös johdon esimerkkiä ja sitoutumista. Perustettavan turvallisuusorganisaation tulee olla kiinteä osa yrityksen johtamisjärjestelmää ja noudattaa kaikin tavoin nykyisiä vakioksi muodostuneita menettelytapoja ja jo olemassa olevaa hierarkiaa.

Turvallisuusorganisaatiossa toimitusjohtaja on turvallisuudesta vastaavan johtoryhmän puheenjohtaja ja esittelijänä toimii turvallisuudesta vastaava henkilö. Johtoryhmään kuuluu yleensä myös muuta yrityksen ylintä johtoa. Jokaisella johtoryhmään kuuluvalla ylemmällä toimihenkilöllä on hoidettavana myös omat erikseen tehtävänkuvausten mukaisesti nimetyt ja vastuutetut turvallisuuden osa-alueet. Linjaorganisaatioon kuuluvat esimiehet toimivat operatiivisesta turvallisuustoiminnasta vastuullisena, siksi heidät on myös tarpeen sijoittaa turvallisuusorganisaatioon, vaikka he eivät toimitukseen tehtäviensä puolesta johtoryhmässä. On myös nimettävä kohdeorganisaatioiden kiinteisiin toimistoihin turvallisuudesta vastaavat ja heidän varahenkilöt, jotka huolehtivat kunkin paikan juoksevista turvallisuusasioista ja jotka ovat esimerkiksi koulutettu toimimaan paloturvallisuuteen liittyvissä suojelutehtävissä. Harkinnan ja toiminnan mukaan tulee myös asiakaskohteisiin nimetä turvallisuusvastaavia henkilöitä.

Ennen kuin turvallisuusorganisaatio muodostetaan, on sen toiminta ja tarkoitus määriteltävä. Perustettavalle turvallisuusorganisaatiolle on määriteltävä olemassaolon edellytykset ja tehtävät, vastuut ja tiedonkulkuun liittyvät seikat, jotka on dokumentoitava. Etukäteen on myös suunniteltava toimintatapamenettelyt erilaisten riskikartoitusten ja turvallisuusuhkien mukaan siten, että johtoryhmä tietää kuka reagoi, tutkii, selvittää, johtaa, ohjeistaa ja tiedottaa. On myös hyvä valmistella viestintäsunnitelma sen varalta, jos joskus joutuu antamaan tiedotteita tai suoraan viestimään medialle yllättävissä poikkeamatilanteissa tai havereista.

Alla esitettyssä kuviossa (kuvio 7) on esitetty yksi auditoijan suunnittelema toteutusehdotus turvallisuusorganisaation toiminnan järjestämisestä siten, että yrityksen turvallisuuden tilannekuva olisi mahdollisimman reaaliaikainen ja poikkeamatilanteissa tärkeät tiedot kulkisivat esteittä ja nopeasti oikeaa rataa pitkin aina päätöksentekoportaalalle asti. Kuviossa hahmotettu nopeasti myös, miten vaikeaa on luoda sellainen toiminnallinen kokonaisuus, joka varmasti toimii työssäoloaikana ja kuinka herkkä se voi todellisuudessa olla ulkoisille häiriötekijöille.

Koska elämme some- ja mediaviestinnän kulta-aikaa oletamme, että kaikilla on jonkinlainen viestintäväline aina mukana. Tämä pitänee yleensä paikkansa, mutta siihen ei pidä silti luottaa varmana asiana. Aina ei saada oikeaa henkilöä heti kiinni, koska tavoitettava henkilö ei muistanut ladata puhelinta tai ei ole juuri sillä hetkellä paikassa, jossa puhelinverkko toimii ja puhelinverkon peittoalueen kuuluvuus olisi riittävän hyvä. Silti on, monesta muustakin syystä, huolehdittava kaikista mahdollisista henkilöihin ja viestintään liittyvistä varajärjestelyistä, joiden päätarkoitus on vain varmistaa tiedonvälitys normaalia poikkeavimmissa tilanteissa.



Kuvio 7: Turvallisuuden organisointi, poikkeamatilanteen tiedonkulku ja tilannekuvan ylläpito

Seuraavissa alaluvuissa esitetään kysymyksen edellä suluissa iso K, M, S, T tai U kirjain, joiden tarkoitus on tuottaa lisätietoa. Lisätiedon antamisella on yritetty helpottaa tai ohjata kysymyksiä koskevaa käsittelyä. Tämä tarkoittaa esimerkiksi sellaista tilannetta, kun kysymyksen mukaisen käsittelyprosessoinnin jälkeen on saatu tehtävä valmiiksi, voidaan silti joutua palaamaan asiaan myöhemmin uudelleen. Osalla kysymyksen mukaisilla tilanteilla tai tehtävillä, on sellaisia ominaisuuksia, joihin tulee uudelleen palata vuoden (S) tai kahden vuoden

välein (T) tai kun on tapahtunut muutoksia (M). Tällä toteutukseen kirjatulla lisäpiirteellä auditoija on kehittämissuosituksissaan halunnut tuoda esille vuosikellon mukaisesti sovellettavia kausitehtäviä, joita tulee aika ajoin tarkastella ja arvioida myös uudelleen ja tarkistaa ettei tilanne ole ratkaisevasti muuttunut tai päivityksen tarpeessa tai on myös sellaisia kysymyksiä, joiden kohdalla on vuosittain tehtävä kokonaan uusi versio (U).

Alla on esitelty alaluvuissa esitettyjen kysymysten eteen lisättyjen kirjainten merkitys:

(K) Kaikkien vastuulla; sitouduttava, seurattava ja jatkuvasti kehitettävä tätä asiaa

(M) Suunnitelma tai pysyväisohje, joka muutoksen yhteydessä hyväksytetään uudelleen.

(S) Toimintasuunnitelma yhdelle vuodelle, jonka toteutusta seurataan kvartaaleittain.

(T) Tarkistetaan tehdyn päätöksen riittävyys joka toinen vuosi (esim. resurssit ja vastuunjako)

(U) Uudelleenarviointi kerran vuodessa (esim. riskienarviointiprosessi)

7.2 Ylin johto

Tähän alalukuun on kerätty turvallisuudesta tehtäviä linjauksia ja päätöksiä, joita vaaditaan, kun tämän raportinmukaisia ehdotuksia aiotaan toteuttaa. Ensin tarvitaan yrityksen ylimmän johdon strategisia kannanottoja ja joukko hyväksymisiä, ennen kuin voidaan edetä turvallisuutta edistävissä ja parantavissa kehitystoimissa. Lista toimii myös toisin päin, jolloin ylin johto tekee päätöksiä, ettei ehdotuslistan mukaan jotakin asiaa toteuteta. Hyväksymisien yhteydessä varmistetaan myös samalla ylimmän johdon sitoutuminen tehtyihin päätöksiin ja täytäntöönpanossa tarvittava tuki sekä ylläpitoon vaaditut resurssit. Tässä alaluvussa ei ole esitetty kaikkia päätettäväksi tuotavia asioita vaan muissa alaluvuissa esitetään myös ehdotuksia, jotka auditoijan käsityksen mukaan kuuluu ensin valmistella muualla.

Esitys ei ota kantaa, kuka viimekädessä päätöksen tekee vaan lähtee siitä olettamuksesta, että yrityksen ylimpään johtoon kuuluu, tilanteen mukaan, joko yksistään päätöksiä tekevä toimitusjohtaja tai hänen lisäkseen myös yrityksen johtoryhmään kuuluvia ylempiä toimihenkilöitä. Se onko kehityslistan esityksistä tehtävä valmisteluja ja kuinka paljon, riippuu tilanteesta, arvioituista puutteiden korjaustarpeista ja kohdeorganisaation päätöksienmukaisista parantamiskohteista. Kaikki tässä raportissa esitetyt kohteet ovat kehitysehdotuksia, jotka on todettu Katakriin mukaan arvioituna tarpeellisiksi ja merkityksellisiksi kehityskohteiksi.

7.2.1 Yrityksen johdon strategiset linjaukset ja päätökset

Ylimmän johdon tekemillä turvallisuutta käsittelevillä strategisilla linjauksilla ja hyväksynnöillä luodaan perusta yrityksen turvallisuustoiminnan ylläpidolle ja taataan turvallisuuden jatkuva parantaminen. Samalla kun tehdään turvallisuutta parantavia tai kehitysehdotuksen mukaisia päätöksiä, ylin johto voi asettaa ja määrittää turvallisuudelle tavoitteita sekä reunaehto-

ja. Päätöksien syntyvaiheessa tulee myös ottaa huomioon, että kaikkiin ratkaisuihin on myös näkyvästi sitouduttava ja niitä on oltava myös aina valmiita tukemaan, niin valmisteluvaiheissa kuin itse toteutuksessa ja tietenkin toiminnan ylläpitämisessä.

Yrityksen ylimmän johdon tehtävät, toimet, päätökset tai ratkaistavat kysymykset:

- (U) Olemme tietoisia yritystä uhkaavista keskeisistä riskeistä, koska olemme säännöllisessä riskienarvioinnin tunnistus-, määrittely-, arviointi- ja luokitustilaisuuksissa mukana?
- (U) Olemme asettaneet eri hierarkiatasolle turvallisuustyön tavoitteita, valinneet toteutusmenetelmiä ja seuraamme sekä arvioimme asetettujen tavoitteiden saavuttamista?
- (M) Hyväksymme allekirjoittamalla yrityksen turvallisuuspolitiikan ja sitoudumme siihen?
- (M) Olemme hyväksyneet ja sitoutuneet yrityksen tietoturvaperiaatteisiin sekä tietoturvallisiin käytänteisiin, joiden toteuttamista tulemme tukemaan ja seuraamaan?
- (M) Olemme määritelleet salassa pidettävän tiedon omistajien vastuut ja käyttöympäristöiltä ja järjestelmiltä vaaditut suojaustoimenpiteet?
- (M) Olemme varmistaneet, että salassa pidettäviä tietoja koskevia velvoitteita noudatetaan tietoja käsitellessä muualla kuin yrityksen sisällä tai hallinnoimassa järjestelmässä?

7.2.2 Yrityksen johdon tekemät vastuunjaot, toimivaltuudet ja resurssit

Yrityksen johdon on annettava realistiset onnistumisen mahdollisuudet, aikaa ja riittävät resurssit, jotta turvallisuustoiminnat pystytään toteuttamaan asetettujen tavoitteiden mukaisesti. Turvallisuudesta vastaavien tulee voida toimia tehtävissään ja rooleissaan riittävin valtuuksin sekä heillä tulee antaa aikaa kehittää kokonaisturvallisuutta ennaltaehkäisevästi.

Yrityksen ylimmän johdon tekemät vastuunjaot, toimivaltuudet ja resurssit:

- (T) Olemme resursoineet riittävästi turvallisuustyöhön, sen johtamiseen, ylläpitämiseen ja seurantaan sekä jatkuvaan ennaltaehkäisevään suunnitteluun ja kehittämiseen?
- (T) Olemme resursoineet riittävästi osaamista ja tietotaitoa tietohallinnon ylläpitämiseksi, jatkuvuuden varmistamiseksi, ulkoistustoimien koordinoimiseksi ja valvomiseksi.
- (T) Olemme varanneet tietoturvallisuuden hallitsemiseksi riittävät resurssit ja asiantuntemuksen sekä varmistaneet resurssien riittävyyden arvioimalla sitä säännöllisesti?
- (T) Olemme varmistaneet, että tietoturvavastaava saa tietoturvapoikkeamatilanteessa nopeasti tiedon tapahtuneesta ja pystyy reagoimaan tapahtumaan suunnitelmallisesti?
- (T) Olemme resursoineet riittävästi ennakoivaan turvallisuuspoikkeamien hallintaan, jolla varmistetaan tehokas toiminta ei-toivotuissa tilanteissa, pystytään palauttamaan nopeasti tilanne normaaliksi asetetun toipumisajan puitteissa ja minimoidaan vahingot?
- (M) Olemme päättäneet tietoturvapoikkeamatilanteiden viestintäkäytännön vastuista?
- (M) Olemme määrittäneet onnettomuuksien, vaaratilanteiden, turvallisuuspoikkeamien ja tietoturvapoikkeamien käsittelystä, tutkinnasta ja viestimisestä vastaavat henkilöt?

7.2.3 Turvallisuuden tilannekuva ja toiminnan taso

Turvallisuustilanteen mukaista tilannekuvaa ylläpidetään seuraamalla ja valvomalla toimintaa. Se voi olla myös osana johtamis- ja raportointiprosessia, mutta organisaation on varmistettava, että tiedonkulku, reagointiajat ja toiminta vastaavat sitä turvallisuustavoitetta ja tasoa, mitä pidetään liiketoiminnan kannalta riittävänä. Samanaikaisesti turvallisuuden toiminnan taso, toimivuutta ja tehoa tulee koko ajan myös arvioida, kartoittaa ja mitata.

Yrityksen ylimmän johdon on oltava selvillä ja tiedettävä, mitä milloinkin tapahtuu:

- (T) Olemme selvillä kokonaisturvallisuuden nykyisestä tilannekuvasta ja toiminnan tasosta sekä varmistaneet myös välittömän raportoinnin huomattavissa poikkeamatilanteissa?
- (T) Toteutamme sisäisiä arviointitarkastuksia turvallisuusjärjestelmien toimivuudesta, soveltuvuudesta, riittävydestä sekä tehokkuudesta ja saadut tulokset dokumentoidaan?
- (T) Olemme varmistaneet, että yrityksessä tunnetaan riittävästi turvallisuustoimintaan liittyvää lainsäädäntöä ja lakien kehitystä sekä muutoksia myös seurataan koko ajan?

7.2.4 Yrityksen toiminnan kannalta tärkeät suojattavat kohteet

Yrityksen ylimmän johdon on tehtävä ratkaisuja ja linjauksia, mitä se katsoo oman toiminnan jatkuvuuden kannalta tärkeimmiksi varmistustoimiksi ja suojattaviksi kohteiksi. Tunnistetuille suojattaville kohteille on määritettävä turvallisuuden ja suojaustoimien tavoitteet ja niistä vastaavat henkilöt. Toiminnan jatkuvuuden ylläpito voidaan varmistaa poikkeamatilanteiden varalle tehtävillä menettelytapaohjeilla ja varautumissuunnittelulla.

Yrityksen johdon on hyväksyttävä toimintaa ylläpitävät suojaukset:

- (M) Olemme hyväksyneet yrityksen turvallisuuspolitiikassa määritellyt keskeiset suojattavat kohteet ja niihin liitetyt suojaus- ja turvallisuustavoitteet?
- (M) Olemme nimenneet suojattaville kohteille turvallisuudesta vastaavat henkilöt?
- (M) Olemme hyväksyneet yrityksen jatkuvuussuunnitelmat, joka varmistavat toiminnan jatkumisen ja riittävässä ajassa tapahtuvan toipumisen?
- (M) Olemme tunnistaneet jatkuvuutta uhkaavat vaarat ja varautuneet niihin suojaus-, varmennus-, vara-, kahdennus-, palautus- ja toipumissuunnitelmin sekä menettelyin?
- (M) Olemme hyväksyneet yrityksen huomattavien poikkeamatilanteiden varalle dokumentoidun toimintatapamallin ja ohjeistukset?
- (M) Olemme sitoutuneet harjoittelemaan erityisen tärkeitä poikkeamatilanteita varten?

7.3 Turvallisuusjohtaminen

Turvallisuuden hallinnollinen ja operatiivinen johtaminen tulisi saattaa järjestelmällisiksi vuosikellomaisiksi systeemeiksi ja prosesseiksi, joilla taataan jatkuva kehittäminen ja nopea reagoititapa muutoksille ja niistä tehtäville päätöksille. Riskienarviointi ja riskien hallinta on yksi tärkeimmistä turvallisuuden prosessimaisesti käyttöönotettavista toimintamalleista, jolla luodaan perusta sekä lähtökohta kokonaisturvallisuuden toteuttamiselle, ylläpidolle, seurannalle ja ennakoivalle jatkuvalla kehittämiselle.

7.3.1 Yrityksen turvallisuuspolitiikka

- (M) Käytän johdon turvallisuusjohtamisjärjestelmästä tehtyjä tarkastusarviointien palautteita turvallisuuspolitiikan ja turvallisuustavoitteiden uudelleenarvioimisessa?
- (T) Laadin turvallisuuspolitiikan tukemaan yrityksen liiketoimintaa, jolla ohjataan turvallisuustoimintaa ja toimii perusteena turvallisuustyön tavoitteiden asettamisessa?
- (U) Olen määritellyt turvallisuuspolitiikassa yrityksen keskeiset suojattavat kohteet, suojaus- ja turvallisuustavoitteet, jotka tarkistetaan johtoryhmässä kerran vuodessa?
- (K) Turvallisuudesta vastaavana valvon ja varmistan, että kaikki organisaatiotasot toimivat turvallisuuspolitiikan mukaisesti?

7.3.2 Riskienhallintaprosessi

Yrityksen kokonaisvaltainen riskienhallintaprosessi

- (U) Teemme yrityksen riskiarviointia säännöllisesti kerran vuodessa tai merkittävän muutoksen tapahtuessa. Riskienarvioinnista saadut tulokset, todennetut riskit ja uhat luokitellaan tärkeysjärjestykseen ja ne dokumentoidaan siten, että ne löytyvät myös helposti? *Suosittelavaa olisi, että yrityksen johtoryhmä kokoontuu kerran vuodessa pohtimaan, tunnistamaan ja päättämään yrityksen toiminnan kannalta tärkeimmistä riskeistä.*
- (U) Käytän riskienarviointia yrityksen turvallisuustyön lähtökohtana ja perusteena. Riskienhallintaprosessin tuloksia olen hyödyntänyt turvallisuustavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, suojattavien kohteiden turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin myös hankintamenettelyissä?
- (T) Katamme riskienarvioinneilla normaalin toiminnan (asiakaskohteet ja konttorit), erityistilanteet ja palvelun toimittajat sekä alihankkijat että sidosryhmät?
- (T) Olen tarkistanut, että riskienarviointi käsittää henkilöstö-, työ-, toimitila-, toiminnan- ja tietoturvallisuuden sekä pelastustoiminnan että valmiussuunnittelun osa-alueet?
- (M) Olen kuvannut käytettävät riskienhallintaprosessit, joilla riskit kartoitetaan ja analysoidaan vakiintuneella, avoimella ja ymmärrettävällä järjestelmällisellä menetelmällä? Käytän seuraavia menetelmiä eri tilanteisiin niiden sopivuuden mukaan:

- Potentiaalisten ongelmien analyysi (POA selvittää keskeisimmät ongelma-alueet)
- Toimintovirheanalyysi (TVA löytää ihmisten toimintovirheistä vaaroja)
- Vaarallisten skenaarioiden analyysi (HAZSCAN soveltuu kemikaalien käytön arviointiin)
- Työn turvallisuusanalyysi (TTA soveltuu työtehtävien tapaturmavaarojen analysointiin)

7.3.3 Turvallisuustavoitteiden määrittely

Yrityksessä on tehtävä suojattavien kohteiden määrittely, tunnistaminen, turvatoimien mitoitukset ja turvajärjestelyiden dokumentoinnit.

- (U) Olen tunnistanut yrityksen toiminnan kannalta kaikki tärkeimmät suojattavat kohteet, järjestelmällisellä menetelmällä, sekä olen arvioinut niihin kohdistuvat riskit ja uhat. Kohdistamani suojaustoimenpiteet on hyväksytty yrityksen johtoryhmässä?
- (T) Huomioin turvatoimien mitoituksessa tiedon suojaustason, määrän, muodon, luokitteluperusteet ja sijoitustilat suhteessa arvioituun uhkaan sekä valitut suojausmenetelmät, jotka olen asianmukaisesti suhteuttanut kohteisiin kohdistuvien riskien mukaan?
- (M) Ylläpidän yrityksessä turvallisuusjärjestelyjen kuvausta ja olen dokumentoinut yrityksessä sovellettavat valvonta- ja turvatoimet?

7.3.4 Kokonaisturvallisuuden suunnitelmallinen hallinta

Turvallisuusjohtamiseen on aikaansaattava suunnitelmallinen, tavoitteellinen ja vuosikellomainen kokonaisturvallisuuden hallintasuunnitelma tai -ohjelma.

- (S) Valvon ja johdan yrityksen turvallisuutta seuraamalla tavoitteiden saavuttamista sekä edistymistä säännöllisesti kvartaaleittain laatimani toimintasuunnitelman mukaisesti?
- (S) Erittelen turvallisuuden toimintasuunnitelmassa turvallisuusjohtamisen, -työn ja -toiminnan menetelmät, vastuuhenkilöt ja aikataulut tavoitteiden saavuttamiseksi?
- (S) Asetan yrityksen turvallisuustavoitteet turvallisuuspolitiikan mukaisesti selkeästi ja ymmärrettävästi sekä esitän tavoitteiden saavuttamisen ja tason realistisilla mittareilla, jotka olen dokumentoinut niin, että niitä voidaan myös jatkuvasti kehittää?
- (S) Huomioin yrityksen turvallisuustoiminnan tavoitteiden asettamisessa
 - tekniset vaatimukset ja mahdollisuudet?
 - yrityksessä tunnistetut riskit?
 - toimialan vaatimukset ja määräykset?
 - muiden intressiryhmien vaatimukset (esim. asiakkaat, viranomaiset)?

7.3.5 Turvallisuuspoikkeamatilanteet

Turvallisuusjohtamisella vaikutetaan turvallisuuspoikkeamatilanteiden hallintaan suunnitelmallisen turvallisuustoiminnan, jatkuvuussuunnittelun ja varautumisen kautta.

- (M) Olen laatinut yritystoiminnan mukaisia jatkuvuussuunnitelmia, joihin on sisällytetty ennalta ehkäiseviä ja korjaavia toimenpiteitä, joilla etukäteen minimoidaan merkittävien liiketoiminnan toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutuksia?
- (M) Olen huolehtinut, että yrityksellä on ohjeistettu, koulutettu, viestitetty ja dokumentoitu toimintamalli, jossa määritellään menettelytavat turvallisuuspoikkeamatietojen tai niiden epäilysten kirjaamisesta, edelleen ilmoittamisesta ja siitä, kuka vastaa tilanneku- van mukaisesta ylläpidosta, tarvittavista jatkotoimenpiteistä, tutkinnasta ja viestinnästä?
- (M) Vien yrityksessä turvallisuuspoikkeamista tehdyt havainnot osaksi riskienarviointia ja tarpeen mukaan näiden pohjalta päivitän toipumis- ja jatkuvuussuunnitelmia.

7.3.6 Kehittämisen vaikutusanalyysit

Turvallisuuden kehittämisessä, parantamisessa ja korjaustoimenpiteissä on muutosten vaikutuksia seurattava ja arvioitava sekä saatuja analyysituloksia dokumentoitava ja raportoitava.

- (M) Seuraan ja arvioin yrityksessä tehtyjen torjunta-, estämis- tai suojaustoimenpiteiden toteuttamista, toimenpiteiden tehokkuutta ja tavoitteiden mukaisia vaikutuksia?
- (M) Huomioin ja varmistan muutoksenhallinnan riskianalyysiarviossa, ettei turvallisuusjär- jelmiä muutettaessa samalla aiheuteta uusia uhkia tai vaaratilanteita. Huomioin, että valitut toimenpiteet ja menetelmät ovat myös tehokkaita sekä oikein kohdistettuja?
- (M) Dokumentoin yrityksessä toteutetut turvallisuustoimenpiteet sekä niiden vaikutukset?

7.4 Henkilöstöhallinto

Henkilöstöhallinnon vastuulle ehdotetaan valmisteleviksi tehtäviksi työsopimusteknisiä turval- lisuustoimintaan liittyviä työnkuvauksia. Johtoryhmän päätöksillä tulisi saada aikaan työteh- tävien vastuiden ja valtuuksien mukaisia tarkennuksia, jotka edesauttavat omilla kirjaamisilla turvallisuusorganisaation järjestäytymistä. Lisättävät tarkennukset työsopimuksissa tai työn- kuvauksissa olisivat tarpeellisia myös turvallisuudesta vastaavien toimihenkilöiden oikeustur- van kannalta. Samalla mainitut kirjaukset toisivat selkeyttä yrityksen turvallisuuden vastuu- ja valtuutuskysymyksiin, jotka osaltaan myös sitouttavat ennaltaehkäisevään toimintaan. Kaikkien turvallisuudesta vastaavien tehtävänkuvaukset

7.4.1 Tehtäväkuvaukset

Henkilöstöhallinto yksilöi ja kuvaa muodollisesti toimenkuvauksissa sekä työsopimuksissa tur- vallisuudesta vastaavien vaikuttamismahdollisuudet ja tehtävät turvallisuusorganisaatiossa.

- (M) Turvallisuudesta vastaavat on nimetty yrityksen turvallisuusorganisaatioon ja henkilön tehtäväkuvauksissa vastuut sekä johtamisvaltuudet on määritetty ja dokumentoitu (joh- taminen, seuranta, valvonta, tiedottaminen ja sitoutuminen jatkuvaan kehittämiseen)?

- (M) Yritys on nimennyt turvallisuuspoikkeamatilanteiden johtamisen vastuut kriisi- ja vaaratilanteiden, onnettomuuksien ja poikkeamien vaikutusten ennalta pienentämiseksi?

7.4.2 Asiakirjahallinto ja luokitukset

Lainsäädännölliset asiat ja henkilötietolain soveltaminen ovat HR -henkilöille entuudestaan tuttuja. Auditoinnin tulosten mukaan nämä asiakokonaisuudet nousivat erityisen korostuneesti esille. Yrityksen turvallisuuskriittisiä puutteita ajatellen tehokkainta ja järkevintä on sijoittaa asiakirjahallinnan ja turvaluokituksen sekä tietosuoja-asioiden käsittelyvastuut samaan yksikköön. Arviolta vuoden 2016 aikana voimaan tuleva EU tietosuoja-asetus koskee myös kohdeorganisaatiota, jossa työskentelee yli 250 henkilöä, jonka mukaan yksi yrityksessä työskentelevä henkilö tulee nimetä tietosuojavastaavaksi. Oletuksena on, että tietosuoja ja henkilötietojen käsittelyosaamisen kautta vastuukokonaisuus luontuu henkilöstöhallinnolle hyvin, ellei luoda vastuukokonaisuutta, jossa on myös tietoturvasuoritusasioita hoitava henkilö.

Asiakirja- ja tietoaineistojen turvaluokitus ja merkitseminen, käsittelyn ohjeistus ja perehdytys, suojaustason mukainen toiminta sekä aineistojen käsittelyä koskeva valvonta

- (M) Yrityksessä käytetään käsiteltävien henkilötietojen ja asiakirjojen turvaluokitusta varustamalla ne suojaustasoa kuvaavalla merkinnällä ja käsittelemällä niitä kansallisten käsittelysääntöjen tietoaineistosta asetettujen vaatimusten ja sopimusten mukaisesti?
- (M) Yrityksessä noudatetaan asiakirjamerkinnästä ja tiedon käsittelystä laadittua ohjeistusta?

Yrityksellä on myös muita suojattavia asiakirjoja ja suunnitelmia kuin esimerkiksi turvallisuusdokumentit. Yrityksessä tiedostetaan hyvin lainsäädännölliset, toimialaa koskevat standardit, tietosuojaan liittyvät velvoitteet ja salassapitosopimukset, mutta onko myös tunnistettu kaikki suojausta tarvitsevat liiketoimintakriittiset tiedot? Liikesalaisuudet, tietopääoma ja erityisosaaminen tai palvelukonsepti on monen yrityksen menestymisen edellytys sekä kilpailutekijä. Oman tiedon merkitystä ei usein oteta riittävästi huomioon tai sitä ei osata oikein tunnistaa tai sitten salaustarvetta ei vain yksilöidä tarkasti. Tiedonkäsittelyssä on huomioitava sekä kriittisen tiedon käsittelyyn liittyvät riskit: kuka, missä ja miten tietoa käsitellään, kuka vastaa ja valvoo sekä miten ja minne tieto tulee suojata. Tiedon käsittelyn ohjeiden puute yhdessä riittämättömän valvonnan kanssa voi johtaa liiketoimintaa vaikeuttaviin yrityssalaisuuksien paljastumisiin tai yrityksen mainetta vahingoittaviin tietovuotoihin.

7.4.3 Lainsäädännön seuranta

Lakien ja asetusten kehityksen ja muutoksien seurannan varmistaminen ja vastuunjako

- (M) Turvallisuuslainsäädännön ja toimialakohtaisten turvallisuusmääräyksiensä sekä velvoitteiden täyttö on varmistettu, päivitetty ja tiedotettu?
- (M) Yritystoimintaa koskevat laki- ja muut vaatimukset on tunnistettu sekä varmistettu, että lakeja seuraa useampi henkilö kuin yksi (esim. vastuujon nimeäminen laeittain)?
- (M) Yrityksen henkilöstön tietoturvarikkomusten käsittely, menettelytavat on määritelty?

7.4.4 Turvallisuuskirjoitusten hallinta

Turvallisuuskirjoitusta syntyy jokaisesta turvallisuuden osa-alueesta, ei pelkästään turvallisuusvastaavan ja työsuojelutoimikunnan tuottamana vaan myös tietohallinnon ja henkilöstöhallinnon tekeminä. Myös eri järjestelmävastaavien toimesta tehdään jatkuvuus ja toimissuunnitelmia, joita voidaan pitää asiakirjan turvaluokitusta ja suojausta vaativina dokumentteina. Peruserä on, että jokainen vastuutaho huolehtii itse kirjoitustaan, mutta on hyvä muodostaa yksi yhtenäinen asiakirjahallinnon ohjeistus, jota noudatetaan.

Turvallisuuskirjoitusten hallintoihin liittyvät vastuut ja ohjeistukset

- (M) Yrityksessä on nimetty ja ohjeistettu turvallisuuskirjoitusten kattavuuteen, ajantasaisuuteen ja seurantaan liittyvät vastuut?
- (M) Yrityksellä on toimintamalli, ohjeistus ja nimetty vastaava, joka huolehtii turvallisuuskirjoitusten arkistoinnista, säilyttämispaikasta ja säilytysajoista?

7.5 Tietohallinto

Tietohallinnossa on tehtävä nopeasti toimintaa selkeyttäviä ratkaisuja ja toiminnan uudelleen arviointia. Samalla on tarkennettava tietoturva sekä tietotekniikan laitteisiin liittyviä vaatimus- ja käyttömäärityksiä että ohjeistuksia. Tietotekniset näkökulmat on huomioitava myös liiketoimintatarpeiden mukaan uudelleen. Vaikka auditoinnissa saatujen tietojen mukaan tietotekniset asiat on ulkoistettu, se ei missään vaiheessa voi tarkoittaa, että myös tietohallinnon vastuu olisi siirretty pois tai ulkoistettu. Näin toimien riskit ja uhkat kasvavat silloin hallitsemattomiksi. Tietohallinnollisia toimintoja ei ole suoritettu niin kuin palvelun hankinnassa tulisi vastuullisesti toimia. On varmistettava, että kaikki toiminta ja tekeminen vastaa myös hyvää tietohallintotapaa ja tietoturvasuoritusvaatimuksia. Koska auditoinnissa ei havaittu, että tietoturvalisten toimintatapojen määrityksiä tai valvontaa olisi mitenkään suunniteltu, järjestelty tai muutoin varmistettu, on nämä asiat otettava heti työlliställe ratkaistaviksi.

7.5.1 Tietohallinnon toimintasuunnitelma ja tietoturvaliiketoiminta

Tietohallinnon ja hallinnollisen tietoturvan organisointi sekä tietoturvaliiketoiminnan määrittäminen

- (U) Yrityksellä on tietohallinnosta määritelty ja dokumentoitu toimintasuunnitelma, tietoturvapoliittikka ja tietoturvasuunnitelma tietoturvallisuuden johtamiseksi sekä tietoturvalisuuden ylläpitämiseksi että asetettujen kehitystavoitteiden saavuttamiseksi?
- (T) Ylin johto katselmoi ja tarkistaa yrityksen hyväksyttävän käytön säännöt, tietoturva-periaatteet ja -käytänteet vuosittain ja aina merkittävien muutoksien tapahtuessa?
- (M) Yrityksen tietoturvaohjeissa on nimetty johdon, peruskäyttäjän, tietohallinnon ja järjestelmävastaavien sekä palveluntoimittajan eli IT -tuen ja ylläpidon vastuut?
- (M) Yrityksestä löytyy dokumentaatiot kuinka tietoturva on hallinnollisesti, teknisesti ja fyysisesti toteutettu?
- (M) Yrityksen tietoteknisiin muutoksiin käytetään omaa muutoksenhallintamenettelyä?

7.5.2 Ulkoistetun palveluntuottajan hallinta

Yrityksen tietohallinnon vastuu kattaa tietotekniikan toiminnan varmistamisen kaikissa olosuhteissa. Auditoinnista saatujen tietojen mukaan tietotekniikan pettämistä pidettiin yhtenä suurimmista ja merkittävimmistä liiketoiminnan jatkuvuutta uhkaavista tilanteista. Jos tietotekniset laitteet, järjestelmät ja tietoliikenne eivät toimi, niin kuinka kauan voidaan liiketoimintaa, palvelusitoumuksia ja asiakassuhteita koko maan kattavalla alueella ylläpitää ja jatkaa? Tärkeää on myös varmistaa, että palveluntuottajalla kaikki toiminta tapahtuu yrityksen etujen mukaisesti, jolloin säilytetään suojatun tiedon saatavuus, eheys ja luottamuksellisuus. Samalla tietojärjestelmien hallinnassa on huomioitava, että ei tapahdu mitään sellaista oikeudetonta toimintaa, johon yritys ei ole antanut lupaa. Kaikki toimeksiannot tulee toimia ehdonalaisesti hyväksymis-, myöntämismenetelmin ja sovituin todennettavissa olevien tunnistuksin, jossa lisäys-, muutos- ja poistotoimet tapahtuvat luotettavasti sovituin menetelmin.

Yrityksen tietohallintovastaavan on hallittava palveluntuottajan toimintaa, varauduttava ja varmistettava että...

- (U) ulkoistettuihin palveluntuottajiin liittyvät riskit on tunnistettu ja niiden mukaan on suunniteltu asianmukaiset turvamekanismit, jotka on toteutettu ja dokumentoitu?
- (U) palveluntuottajan kanssa on tehty sopimus raportoida säännöllisestä tietoturvallisuuden tilasta sekä tilatuille palveluille on sopimuksessa määritelty palvelun laatutaso?
- (U) ulkoistetun palveluntuottajan kanssa on suunniteltu, sovittu ja dokumentoitu tietoturva-epäilyjen varalle omat toiminta- ja menettelytavat?
- (M) kaikki tietoverkot ja -järjestelmät ovat tietoturva-periaatteiden mukaisesti suojattuja?
- (M) suojattuun tietoon ei ole luvatonta pääsyä verkon kautta?
- (M) ulkoistetun palveluntuottajan kanssa on tehty sanktoidut salassapitositoumukset, jolla palveluntuottajayrityksen henkilöstö sidotaan salassapitosopimuksen piiriin?

7.5.3 Tietohallinnon käyttöoikeuksien hallinta

- (M) Yrityksen tietojenkäsittelylle ja järjestelmille on määritelty pääsynhallintapolitiikka, käyttöoikeuksien myöntämismenettely, nimetyt valtuudet ja vastuut tarkistus- ja seurantamenettelyille sekä varmistettava, ettei vaarallisia työyhdistelmiä synny?
- (M) Yrityksessä käytetyn asiakirjaluokituksen mukaan pystytään mitoittamaan suojaustarpeet ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet?

7.5.4 Tietoturvaohjeistukset

Yrityksen tietoturvaohjeet on laadittu tietoturvanäkökulmasta sekä dokumentoidut tietoturva- ja käyttöohjeet löytyvät...

- (M) sähköpostin, internetin ja etäyhteyden käytölle?
- (M) tietokoneiden, kannettavien, tablettien ja puhelimien käytölle?
- (M) tärkeimpiin toimintatilanteita (toimisto, asiakaskohde ja etäkäyttö) varten?
- (M) joiden mukaan yrityksen tarjouspyyntöihin voidaan liittää aina tietoturva vaatimukset?

Ja lisäksi...

- (M) On huolehdittu riittävästä ohjeiden mukaisesta koulutuksesta ja tiedottamisesta?
- (M) Edellytetään, että kaikki työntekijät, toimittajat ja myös ulkopuoliset tietojen käsitteijät toimivat yrityksen tietoturvaperiaatteiden mukaisesti?

7.5.5 Tietoturvapoikkeamien hallinta

Tietoturvapoikkeamat vaativat oman hallintamenettelynsä ja osaavan tietoteknisen asiantuntijan arvioimaan tapahtuneiden poikkeamien ja uhkien vaikutusta sekä merkittävyyttä. Tämä voidaan myös toteuttaa yhteistoiminnassa ulkoistetun palveluntuottajan kanssa sopimuksessa edellytetyllä tavalla sekä sovittuja toimintatapoja noudattamalla.

- (U) Tietohallinto on ohjeistamalla ja kouluttamalla varmistanut, että tietoturvapoikkeamatilanteissa tieto heti välittyy nimetyille vastuuhenkilölle, jotta voidaan nopeasti reagoida ennalta suunnitelluin suojaus-, torjunta- tai palautustoimilla.
- (M) Yrityksessä on suunniteltu tietoturvapoikkeamien hallinta ja tietojen tallennus sekä dokumentoitu menettelytavat, jotta havaintoja voi tuoda myös osaksi riskien arviointia?
- (M) Yrityksen ja tietohallinnon jatkuvuussuunnitelmissa huomioidaan tarve suojata tiedot hätätilanteissa, jolloin estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai käytettävyyden menettäminen?

7.6 Linjaorganisaatio

Linjaorganisaatiolla tarkoitetaan sellaista esimies, työnjohto ja työnhajaaja joukkoa, jolle lankeaa suurin vastuu turvallisuuden operatiivisesta toteutuksesta, valvonnasta, perehdytyksestä, kouluttamisesta ja viestinnästä. Kirjaimellisesti tämä on se toiminnan taso, jonka on viimeistään varmistettava, että turvallisuutta käsittelevät aiheet, ohjeet, lait ja määräykset tulevat kaikille ymmärrettävästi informoiduksi sekä jaetuksi että toteutetuksi. Tämän toiminnan onnistunut toteutuminen ratkaisee sen, miten turvallisuutta ja turvallisuuskulttuuria pidetään yllä ja millä tavalla turvallisuuden kulttuuri itse toiminnassa todellisuudessa kehittyy.

Turvallisuuskulttuuri toteutuu parhaiten pitkäjänteisellä työllä, huolehtimalla asioiden tilasta, toimimalla esimerkkinä ja sitoutuneella asenteella sekä jatkuvalla valvonnalla. Turvallisia toimintatapoja ja käytäntöjä sekä ohjeiden mukaista toimintaa ei saavuteta, ellei sitä myös seurata, arvioida ja kehitetä jatkuvasti koko ajan. Kaiken lähtökohtana on toteuttaa perehdytykset ja koulutukset tasaisesti ja siihen esitettynä ratkaisuna koulutusvideot ovat erinomainen keksintö, johon kannattaisi panostaa ja joiden toteuttaminen ei ole enää nykytekniikalla vaikeaa. Perusteellisesti ja loppuun saakka suoritettujen opastuksien tavoitteena on, että niiden jälkeen voidaan olettaa jokaisen työntekijän ymmärtäneen turvallisuuden merkityksen ja ohjeiden noudattamisen tärkeyden. Eteen tulee myös tilanteita, jolloin on asioita otettava uudelleen esille, toistettava ohjeita ja kerrattava koulutusasioita. Linjaorganisaation vastuulla on viimekädessä kaiken turvallisuustiedon sekä asioiden perillemenon varmistaminen. Samalla kun perehdytykset, koulutukset ja tiedottamiset on toteutettu, on varmistettava, että tapahtumat ovat myös heti kirjattu huolellisesti koulutusrekisteriin.

7.6.1 Perehdytys-, koulutus-, seuranta-, valvonta- ja tiedottamisvastuu

Turvallisuuskoulutuksen tason tasaisuuden varmistaminen seurannalla ja valvonnalla

- (K) Yrityksen kaikki henkilöt ovat tietoisia turvallisuusvaatimusten noudattamisen tärkeydestä, oikeista ja hyväksytyistä toimintatavoista?
- (K) Yrityksen koko henkilöstö on perehdytetty ja koulutettu turvavaatimusten mukaan ja on huolehdittu, että kaikki koulutustiedot on kirjattu, myös asiakaskoulutukset?

Linjaorganisaation vastuulla ja tavoitteena ovat:

- (K) Yrityksen turvallisuuspolitiikka, turva- ja tietoturva-periaatteet, yleiset turvallisuusohjeet ja kohdeohjeet, jotka ovat perehdytetty, koulutettu ja tiedotettu kaikille työntekijöille ja ne ovat myös jatkuvasti kaikkien saatavilla ja nähtävillä?
- (K) On varmistettu, että kaikki yrityksen työntekijät tietävät, kuinka toimia turvaohjeiden mukaisesti ja ymmärtävät varmasti turvallisuuteen liittyvät vastuunsa ja velvollisuutensa?
- (K) Yrityksen työntekijät ovat sitoutuneet jatkuvaan turvallisuustilanteen parantamiseen?

Linjaorganisaation vastuulla on johtamiseen kuuluvana työnä tuntea turvallisuus- ja tietoturvapoliittikka sekä seurata ja valvoa niiden toteutumista

- (K) Yrityksessä turvallisuuden ja tietoturvallista toimintatapaa, käytäntöjen toteutumista ja noudattamista valvotaan ja seurataan sekä rikkeisiin puututaan välittömästi?
- (K) On varmistettava, että kaikki työntekijät todella tietävät varmasti, miten poikkeamatilanteissa toimitaan oikein ohjeiden, ilmoitusvelvoitteiden ja toimintatapojen mukaan.
- (K) Yrityksen turvallisuus- ja tietoturvaohjeita arvioidaan ja kehitetään jatkuvasti?
- (K) Tietoturvapoikkeamista ja havainnoista lähetetään ilmoituksia tietoturvavastaavalle?

7.6.2 Poikkeamatilanteisiin varautuminen

Varaudutaan toimimaan oikein poikkeamatilanteissa

- (K) Yrityksen jokainen työntekijä tietää turvallisuusorganisaatiossa toimivien roolit ja vastualueet, jonka mukaan tiedetään kenelle ilmoitetaan, missäkin ongelmatilanteessa ja keneltä saa ongelmatilanteeseen apua ja tukea?
- (K) Turvallisuusorganisaatio (tuleva!) on koulutettu ja tiedotettu koko henkilöstölle. Tiedot ovat myös saatavissa päivitettyinä tietojärjestelmästä sekä kohdekansiossa?
- (K) Varmistettava, että poikkeamatilanteissa tieto kulkee vähintään esimiehelle.

7.7 Asiakkuudenhallinnassa turvallisuusnäkökulman parantaminen

Tämä on toiveesta lisätty innovointiosuus ja jatkokehittämisaalue, jonka tarkoitus on herättää keskustelua siitä, millä tavalla voitaisiin kääntää turvallisuuteen sijoitetut panostukset myös liiketoiminnan hyödyksi ja myytävän palvelutuotteen lisäarvoksi tai jopa hyvin tuotteistettuna kilpailutekijäksi, vaikka turvallisuusosaamisesta ei erillistä myytävää lisätuotetta voisiakaan muovata. Lähtöajatus on, että asiakaskohteessa tehtyä turvallisuustyötä voitaisiin käyttää muuhunkin kuin vain omiin tarpeisiin, esimerkiksi työturvallisuusvelvoitteiden täyttämiseen.

Ostetun palvelun tulee tyydyttää asiakastarpeet, mutta enenevissä määrin asiakasyritys kiinnittää huomiota alihankkijoidensa turvallisuusasioiden hoitoon ja tasoon arvioidessaan tulevia yhteistyökumppaneja. Koska palvelut ja niiden tuottaminen tulee olla turvallisia, niin miksei siihen myös silloin riittävästi ja näkyvästi panosteta, jos sitä voidaan myös käyttää markkinoinnin apuna. Palveluideana turvallisuutta voi tehdä asiakkaalle ymmärrettäväksi helposti tarjous- ja sopimusneuvotteluissa. Koska turvallisuus on osa tuotettua kokonaispalvelun laatua, se myös määrittää osaltaan laadun ja kuinka laadukkaaksi asiakas saadun palvelun kokee. Työtapaturmien aiheuttamat tilanteet, seuraamukset ja viivästymiset eivät ole niitä asiakkaalle mieluisia tilanteita, kun toivotaan sujuvaa, häiriötöntä ja turvallista palvelutoimintaa.

Auditoinnista saatujen tulosten perusteella, yrityksessä X on viimeisen kahden vuoden aikana, tehty onnistunut palvelutuotannon parantamisoperaatio. Toteutettu laaja palvelukonseptin yhteyteen kuuluva turvallisuuskoulutus on vaikuttanut, tapaturmatilastojen mukaan, tapaturmien ja haverien huomattavaan vähentymiseen. Jo tämä todistettavissa oleva tapaturmatilastotiedon muutos ja kehityssuunta on yksi markkinointiin liitettävä yksityiskohta, jota tulisi hyödyntää. Tätä markkinointihyötynäkökohtaa ei tule väheksyä, sillä viime vuosien aikana on yhä enemmän alettu kiinnittää huomiota yritysten moraalisten ja eettisten arvojen mukaiseen toimintaan. Tasokasta työturvallisuuden hoitoa pidetään yhtenä osaavan ja laadukkaasti hoidetun yritystoiminnan merkinä. Syystä, että kaikki häiriötilanteet ja vahingot aiheuttavat kustannuksia, tuotantokatkoksia ja heikentävät kannattavuutta, jossa yhden yrityksen puutteet ja vaikeudet voivat heijastua toisiin alihankkijoihin ja sitä kautta päätoimijaan asti.

Uudempi ajatus lähtee kuitenkin olettamuksesta, että ainakin osalla henkilöistä on muodostunut hyvä kokemus ja ammattitaito huomaamaan työhön liittyviä turvallisuusuhkia ja -riskejä. Olkoonkin tämä asiantuntija esimies, ohjaaja tai suorittavan työn tekijä, hänellä on kehittynyt silmää turvallisuuden näkökulmasta asioille, joita hän jokapäiväisessä työssä kohtaa. Tätä luontaista tai harjaantunutta taitoa voisi hyödyntää paremmin. Lisäksi tietoa lisäämällä ja kehittämällä voitaisiin saada myös lisäarvoa sille palvelutyölle, jota asiakaskohteissa tehdään jo nyt pelkästään olemalla ainoana henkilönä paikan päällä tekemässä havaintoja.

Panostamalla turvallisuusosaamiseen, kehittyneen ja lisääntyneen tietotaidon myötä voi myös saada aikaan muuta hyötyä ja lisäarvoa. Samalla kun työntekijöiden turvallisuutta ja palvelutuotannon turvallista toimintaa parannetaan, voidaan saatua kokemusta myös käyttää laajemminkin asiakkaan hyödyksi. Työturvallisuuslaissa veloitetaan, että päätoimijalla eli asiakkaalla on tiedotus- ja varmistamisvelvollisuuksia pelastustoimesta, toimintaohjeista ja turvallisuudesta työympäristöstä sekä niiden olosuhteista. Olisi hyvin luonnollista, että kaikki kentällä tehty havainnointi, jota ei aina edes asiakas itse päätoimijan ominaisuudessa ja velvollisuuksistaan huolimatta näe tai kuule, tulisi käytettyä optimaalisesti hyväksi. Yrityksen X työntekijöiden ja erityisesti esimiesten toimiessa asiakaskohteissa ”ylimääräisenä turvallisuudesta vastaavana” tulisi miettiä perusteellisesti turvallisuuskoulutuksen näkökulmasta, miten tätä asiakkaiden laiminlyömiä aukkoja voitaisiin paikata ja samalla omaa palvelutasoa lisätä.

Kokonaispalvelukonseptin kehittämisenäkökulmasta voidaan ajatella, että samalla kun riskien arviointia asiakkaan kohteissa ammattitaidolla tehdään ja säännöllisesti vuosittain päivitetään, arviointityön tulosta olisi hyvä saada hyödynnettyä myös muutoin. Riskilähtöisen arvioinnin mukaan käytävän vuoropuhelun ja vaikuttamisen yksi tarkoitus on kokonaisvaltaisesti parantaa kohteen turvallisuutta, ei pelkästään omien työntekijöiden työtehtäviin liittyvien suoritusten osalta. Kun toteutuneita tilanteita seurataan paikan päällä ja tehdään koko ajan havaintoja, on sillä oltava vaikutusta erityisesti sellaisissa kohteissa, joissa ei ole panostettu

yhtään mitään tai turvallisuusasioiden huomiointi on osittain sivuutettu. Näin voidaan saada aikaan tiiviimpi yhteistyö, kumppanuus ja tilanne, jossa turvallisuutta saadaan parannettua.

Auditointituloksissa oli huomioitavissa ongelmatilanne, jossa kohteessa ei ole tehty minkäänlaisia turvallisuusjärjestelyjä, mikä aiheellisesti lisää työntekijöiden turvattomuuden tuntua. Ottamalla aloitteellisen ja aktiivisen roolin asiakaskohteiden palvelutapahtumassa, voidaan luoda uusia myyntiä edistäviä aluevaltauksia ja tuoda palvelulle lisäarvoa. Asiakasyhteistyön tuotavaa turvallisuuden kehittämistä ja ylläpitoa voidaan perustella kokemuksella ja lakin mukaisilla veloitteiden täyttämällä. Pelastuslaissa ja asetuksissa on monia sellaisia yrityksen X asiakaskohteisiin kuuluvia pykäläitä, joiden hyvä hallinta voi luoda lisäarvoa ja -työtä, kun työn ohessa seurataan turvallisuusjärjestelyjen nykytilannetta, autetaan selvittämään lain ja asetusten mukaisia puutteita ja tarjoudutaan korjaamaan nämä veloitteet.

Kaikkia asiakasyhteistyön lisäämistä edistäviä keinoja ja vaikuttamisen osa-alueita tulee käyttää, parantaa ja kehittää. Palvelutuotteille markkinoitavaa lisäarvoa voidaan parantaa juuri asiakaskohteissa sillä, että tekee turvallisuustyötä ja osallistuu aktiivisesti turvallisuuden parannus- ja kehitystyöhön. Asiakaskohteissa aktiivinen ote turvallisuusasioissa voi muodostua myös kilpailutekijäksi. Samalla voidaan varmistaa kokonaisturvallisuuden oikean suuntainen kehitys asiakaskohteissa, joka vaikuttaa sekä omien, että muiden työntekijöiden turvallisuuden paranemiseen. Aktiivisessa roolissa voi onnistua myös vaikuttamaan asiakaskohteissa järjestettäviin turvallisuuskoulutuksiin ja osallistumaan niihin.

Auditoinnista saatujen tietojen mukaan yrityksellä X on sellaisia asiakkaita, jotka olettavat yrityksen X työntekijän, tekevän yksin asiakaskohteen evakuoinnin. Aktiivisessa roolissa toimiva turvallisuusosaamista omaava yrityksen X työntekijä tai esimies voi saada ohjattua ja muutettua kohteen turvallisuusjärjestelmiä ja toimintoja siten, että mahdollinen uhkaava vaaratilanne ei jäisi vain yhden yrityksen X työntekijän varaan ja vastuulle.

Turvallisuuden hallinta on haastavaa organisaatioissa, joissa toimii monia eri toimijoita. Turvallisuuden varmistamiseksi on silloin tärkeää, että kaikki osapuolet tietävät omat roolinsa ja tehtävänsä. Jos asiakas ei ole tehtävänjakoa vielä toteuttanut, on silloin yksi potentiaalinen vaikuttamismahdollisuus ja asiakasyhteistyön lisäämiskeino löydetty. Kohteen yhteistyön vahvistamiseksi voi silloin pyrkiä esimerkiksi siihen, että luo oman ehdotuksen poikkeamatilanteita varten toimivasta tehtävienjaosta ja pelisäännöistä. Luomalla omat tehtäväpuitteet poikkeustilanteita varten ja vaikuttamalla suotuisasti turvallisuustoiminnan kehitykseen asiakaskohteessa, saadaan myös samalla lisäoppia ja kokemusta turvallisuuden kokonaishallinnasta.

8 Johtopäätökset

Nykypäivän yritysturvallisuutta ei enää ylläpidetä sillä, että asiat ovat järjestyksessä ja jokaiseen tilanteeseen on kirjoitettu toimintaohjeet, varoitukset tai kiellot. Toteutuakseen käytännön toiminnassa turvallisuus vaatii, hallinnollisten toimenpiteiden lisäksi, aina myös johdon sitoutumista, läsnäoloa ja valvontaa. Turvallisuutta ei ylläpidetä pelkästään työturvallisuuslakien täyttämällä ja tapaturmatilastoja seuraamalla. Yrityksen turvallisuutta ei ylläpidetä, jos turvallisuusasioihin kiinnitetään huomiota vain silloin, kun on aikaa. Yritysturvallisuuden ylläpidon toteutuminen taataan vain jakamalla riittävästi resursseja ja realistiset onnistumisen mahdollisuudet luodaan, kun jatkuvalle kehittämiselle annetaan riittävästi aikaa.

Tässä työssä tuloksien mukainen nykytilanteen heikkous johtui yksinomaan siitä, että kohdeorganisaatiossa keskityttiin pääosin työturvallisuuteen ja tapaturmien vähentämisen mukaisiin ratkaisuihin. Kohdeyrityksestä saadut auditointitulokset osoittivat, että kokonaisturvallisuudesta havaitut merkittävimmät epäkohdat johtuivat turvallisuudesta vastaavien henkilöiden ajan ja resurssien puutteesta. Toiminta käsitti hyvin hoidettuna työ-, henkilö- ja tilaturvallisuuden ratkaisut. Palo- ja pelastustoimintojen tarkasteluun oli myös kiinnitetty erityishuomiota asiakaskohteissa. Yrityksen kokonaisturvallisuuteen kuuluu kuitenkin kaikki kymmenen turvallisuuden osa-alueita, jota ohjataan turvallisuusjohtamisella. Turvallisuuden osa-alueiden merkityksen ja tärkeysjärjestyksen määrää yrityksen toimiala ja sisäiset strategiset päätökset. Kaikkia turvallisuuteen liittyviä asioita tulee katsoa aina riskilähtöisesti ja kokonaisvaltaisesti ”helikopteri” näkökulmasta. Turvallisuus tulee olla integroituna osana kaikkea muuta toimintaa ja erityisesti sen on oltava vahvasti läsnä yrityksen toimintakulttuurissa.

8.1 Hallinnollisen turvallisuuden auditointi

Ensimmäinen tämän työn tavoite oli selvittää ja tunnistaa kohdeorganisaation hallinnollisesta turvallisuudesta löytyviä epäkohtia ja puutteita. Tutkimuksen ja itse auditoinnin aikana pääongelmaan ja kysymykseen saatiin kerättyä paljon vertailutietoa sekä tietoaineistoa. Auditoinnissa käytettyjä tiedonkeruumenetelmiä voidaan pitää pääosin onnistuneina valintoina, koska opinnäytetyössä saatiin luotua itse päätavoitteen mukainen kehittämis ehdotus. Erityisenä onnistumisena voidaan pitää erityisesti sitä, että Katakryn auditointituloksien mukaan löydetyt epäkohdat voitiin järjestää ja jakaa kohdeorganisaation vastuujon mukaisiin kehittämisaihe-alueisiin. Kehittämis ehdotuksessa käytetyllä vastuujalla oli tarkoitus nopeuttaa kehittämis tehtävien aloittamista, jakamalla toteutusten käsittelyyn tarvittavia resursseja.

Auditointityössä toteutettu kvantitatiivinen osa turvallisuuskyselystä osoittautui luotettavuuden osalta kyseenalaiseksi. Tämä johtui siitä, että auditointi ei onnistunut muokkaamaan tai muotoilemaan kaikkia kysymyksiä riittävän ymmärrettäviksi ja selkeiksi. Ymmärrettävyyteen

vaikutti osaltaan lauseiden monimutkaisuus tai käytetty turvallisuusalan termistö, joka ei ollut kaikille vastaajille tuttu. Mahdollisista vääринymmärryksistä syntyneet epäselvyydet näkyivät myös tuloksien ristiriitaisuuksissa. Suurimmat eroavaisuudet havaitaan, kun tuloksia verrataan vaatimuskriteeristöstä saatuihin poikkeama-arvioinnin tuloksiin. Turvallisuuskyselyn tulokset osoittautuivat pääosiltaan samankaltaisiksi tai vähintään samansuuntaisiksi tulkinnoiksi kuin mitä arvioinneissakin oli päädytty. Esitetty ja havaittu epäily johti kuitenkin siihen, että kyselyn vastauksia ei täydeltä osuudelta käytetty tulosten arvioinnissa.

8.2 Katakriin soveltuvuus auditointivälineeksi

Tässä tutkimuksessa asetettiin toiseksi tutkimusongelmaksi selvittää Katakriin auditointiprosessin ja kriteeristön soveltuvuus tai jokin Katakriin osan käyttökelpoisuus kohdeyrityksen sisäiseksi turvallisuusjohtamisen kehittämis- ja auditointivälineeksi. Toteutettu esiauditointi kohdeorganisaatioon antoi selkeän kuvan Katakriin ominaisuuksista, mahdollisuuksista ja hyödyistä. Tässä työssä sai hyvän käyttökokemuksen Katakriin auditoinnin ja kriteeristön vaatimusten toimivuudesta, sovellettavuudesta, käytettävyydestä ja siihen liittyvistä ongelmista.

Auditointikokemus osoitti, että kohdeorganisaatiota koskevat esiselvitykset on tehtävä huolellisesti. Auditoidjalle on ensimmäisten tehtävien joukossa tärkeää myös, että Katakriin kysymykset eli vaatimuskriteerit pilkotaan ja puretaan osiksi. Yksilöllisten kriteerien osien erottelu, muokaus, seulonta ja yhdisteleminen on pakko tehdä, koska muutoin ei tiedetä esimerkiksi, mitä dokumentteja pitää tarkastaa ja mitä kriteereitä tulee saada arvioituksi. Tämä on ehdottomasti Katakriin huonoin puoli ja työvälineen käytön kannalta suuri epäkohta. Katakriin mukaista auditointiprosessin suunnittelua ei voi myöskään toteuttaa edellä mainituin syin, jos ei tiedetä etukäteen tarkasteltavaksi vaadittavien kysymysten listaa, jonka mukaan tarkastuksia kohdennetaan ja minkä mukaan poikkeama-arvioinnit suoritetaan.

Onnistuakseen Katakriin mukaisessa auditointiprosessissa, auditoidijan on samalla, kun tutustuu organisaation toimintaan, perehdyttävä huolellisesti itse kriteeristöön esitettyihin tasovaatimuksiin. Vasta riittävän perehtymisen perusteella voi auditoidija tulkita kriteeristön mukaisia vaatimuksia siten, että niistä voi johtaa esimerkiksi tarkasteluun tarvittavat dokumentaatiot. Kriteeristön vaatimuksiin perehtymisen yhteydessä tulee laadittua samanaikaisesti ne tarpeelliset kysymykset, joihin varsinaisen auditoinnin aikana etsitään arvioitavia vastauksia. Ongelma poistuu auditoidijalta silloin, kun asiantuntija on suorittanut useita auditointiohjelmia. Kokenut auditoidija rakentaa tarkastettavien dokumentaatioiden toivelistan aikaisemmin laatimistaan listoista nopeasti. Kohteen yleisilanteen hahmottamis- ja perehtymisvaiheen jälkeen aikaisempia listoja muokkaamalla, kokenut auditoidija voi muodostaa nopeasti kohdeorganisaation yhteyshenkilölle annettavan dokumentaatiolistan, jota halutaan tarkastella ja arvioida.

Toinen ongelma on, että Katakrista ei ole vuoden 2010 jälkeen julkaistu käyttöohjeistusta kriteeristön suositusosuudesta (Kesäläinen 2010). On huomioitava, että pääauditoijille on Katakri II:n mukaan suotu paljon harkinnan ja tulkinnan suhteen pelivaraa päättäessään, mitkä asiat ovat auditointikriteeristön mukaan merkityksellisiä. Selkeänä epäkohtana Katakrien käytölle muodostaa kiinteiden ja virallisten kriteeristöä johdettujen vaatimuslistojen puuttuminen. Näiden virallisten listojen tulisi sisältää kaikki auditoinnissa tarkastettavat turvallisuusdokumentaatiot ja kriteeristön tasovaatimuksista johdetut strukturoidut kysymykset. Listat ja strukturoidut kysymykset mahdollistaisivat tasapuolisemmat sekä yhtenäisemmät lähtökohdat suositusten tarkastelemiselle ja viranomaisvaatimusten täyttämisprosessille.

Jos kohdeyritys ei ole turvallisuuskriittinen toimija eikä osallistu kansainvälisesti kriittiseen tarjouskilpailuun tai hankkeisiin, voi auditoija päättää laajemminkin monista kriteeristöä koskevista asioista. Siten Katakria voi hyvin suositella yksityisen yrityksen auditointivälineeksi, koska se on muokattavissa ja muunneltavissa myös muuhun kuin turvallisuusluokittelun tiedon oikean käsittelyn varmistamiseen ja turvallisuustason tarkastamiseen. Katakri II versiosta ja uudesta 2015 mallista voi yhdessä tai erikseen halutessaan muokata eritasoisia ja käyttökelpoisia, tilanteeseen sopivia sekä kohdennettuja turvallisuuden kehittämiseen tähtäviä tai vain toiminnan tasoa tarkastelevia tarkastuslistoja, koska kriteeristö sisältää hyvät vaatimusten mukaiset kysymykset, joiden mukaan vertailua nykytilan ja tavoitetilan välillä voi suorittaa ja toteuttaa. Oman kokemukseni mukainen arvio on, että Katakri on hyvä ja käyttökelpoinen kohdeorganisaation käyttöön tarkoitettu turvallisuuden auditointiväline. Huomioitavaa kuitenkin on, että Katakri vaatii paljon aikaa esivalmisteluun, perehtymiseen ja suunnitteluun ennen kuin auditointiohjelma on valmis tai auditointiprosessia on edes aloitettu.

8.3 Oman työn arviointi

Oppimiskokemuksena tämä opinnäytetyö edusti Laurean kehittämää kehittämispohjaista oppimismallia (Learning by Developing, LbD). Työssä joutui itse myös kehittämään metodeja, muokkaamaan kysymyksiä ja samalla yhteistyössä kohdeorganisaation yhteyshenkilön kanssa miettimään asiakokonaisuuteen liittyviä kausaalisia ja merkitsevyystekijöitä päämäärän ja asetetun tavoitteen saavuttamiseksi. Itse opinnäytetyöprosessi oli mielekäs, mutta työläs kehittämisen ja toteutuksen sekä aikataulutuksen suhteen. Kokonaisuutena ongelmat ja hyödyt kuitenkin muodostavat arvokkaan oppimiskokemuksen, jota voi hyödyntää myöhemmissä työelämän haasteissa sekä kehitysuunnittelussa. Lopuksi haluan myös kiittää kaikkia tähän työhön osallistuneita yrityksen X turvallisuudesta vastaavia henkilöitä. Yhteistyö oli antoisaa, tehokasta ja ongelmatonta, joka osaltaan helpotti tämän työn toteuttamista ja tekoa.

Lähteet

- Carter, N. 2004. *Auditointi ja ISO 19011*. Helsinki: Gummerus Kirjapaino.
- Flink, A-L., Reiman, T. & Hiltunen, M. 2007. *Heikoin lenkki - Riskienhallinnan inhimilliset tekijät*. Helsinki: Edita Prima.
- Gray, I. & Manson, S. 2000. *The Audit Process - Principles, practice & cases*. Second edition. London: International Thomson Business Press.
- Green, D. 1997. *ISO 9000 Quality Systems Auditing*. Hampshire: Gower publishing limited.
- Hanén, T. 2005. *Turvallisuusjohtaminen ja rajavartiolaitos: Yksittäisten onnettomuuksien tutkinnasta strategisten häiriöiden hallintaan*. Maanpuolustuskorkeakoulu, johtamisen laitos. Julkaisusarja 1, tutkimuksia N:o 30.
- Heinonen, Keinänen & Paasonen. 2013. *Turvallisuustutkimuksen tekeminen*. Helsinki: Tietosanoma.
- Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. *Tutki ja kirjoita*. 13. - 14., osin uudistettu painos. Helsinki: Tammi.
- Katakri II. 2011. *Kansallinen turvallisuusauditointikriteeristö*. Helsinki: Puolustusministeriö.
- Katakri 2015. 2015. *Kansallinen turvallisuusauditointikriteeristö*. Helsinki: Kansallinen turvallisuusviranomainen (NSA).
- Kerko, P. 2001. *Turvallisuusjohtaminen*. Jyväskylä: PS-kustannus
- Kojo, J. 2013. *Viranomaisyksikön turvallisuusjohtamisen tason todentaminen KATAKRIn avulla*. Opinnäytetyö. Espoo: Laurea-ammattikorkeakoulu.
- Kuusisto, A. 2000. *Safety management systems. Audit tools and reliability of auditing*. Väitöskirja. VTT Publications 428. Espoo: Valtion teknillinen tutkimuskeskus (VTT).
- Lanne, M. 2007. *Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa*. Väitöskirja. Tampereen teknillinen yliopisto, tuotantotalouden osasto. VTT Publications 632. Espoo: Valtion Teknillinen Tutkimuskeskus.
- Levä, K. 2003. *Turvallisuusjohtamisjärjestelmien toimivuus: vahvuudet ja kehityshaasteet suuronnettomuusvaarallisissa laitoksissa*. Väitöskirja. TUKES-julkaisu 1/2003. Helsinki: TUKES
- Mäkinen, K. 2007. *Organisaation strateginen kokonaisturvallisuus*. Helsinki: Edita Prima Oy.
- Miettinen, J. E. 2002. *Yritysturvallisuuden käsikirja*. Helsinki: Talentum Media.
- Moilanen, T., Ojasalo, K. & Ritalahti, J. 2009. *Kehittämistyön menetelmät*. Helsinki: WSOYpro.
- Moisio, J & Tuominen, K. 2008. *Laatua ja luotettavuutta ISO 9001. Itsearviointien työkirja*. 57 hyvää kysymystä ja esimerkkiparia. Turku: TS-tulostus / Digipaino.
- Niemelä, M. Pirker, A. & Westerlund, J. 2008. *Strategiasta tuloksiin - tehokas johtamisjärjestelmä*. Helsinki: WSOYpro
- Paasonen, J. (toim.), Huuromonen, T. & Paasonen, L. 2012. *Oppilaitoksen turvallisuusjohtaminen*. Helsinki: Tietosanoma.

Rasmussen, J. 1997. Risk Management in a Dynamic Society: A Modelling Problem. Safety Science 27.

Reason, J. 1997. Managing the risks of organizational accidents. Iso-Britannia: Ashagate publishing Ltd.

Reiman, T. & Oedewald, P. 2008. Turvallisuuskriittiset organisaatiot. Helsinki: Edita Publishing.

Simola, A. 2005. Turvallisuuden johtaminen esimiestyönä. Väitöskirjatutkimus. Oulu: Oulun Yliopisto.

Sjöholm, K. 2010. Turvallisuuden nykytilan kartoitus palvelualan yrityksessä. Diplomityö. Tampere: Tampereen teknillinen yliopisto.

SFS-EN ISO 19011. 2011. Johtamisjärjestelmän auditointiohjeet. Standardi ISO 19011. 2. painos. Suomen standardisoimisliitto SFS. SFS: Tuloste.

Työturvallisuuslaki 23.8.2002/738.

Valtiovarainministeriö. 3/2007. VAHTI - Tietoturvallisuudella tuloksia. Helsinki: Edita Prima.

Sähköiset lähteet:

Elinkeinoelämän keskusliitto. 2015. Yritysturvallisuuden osa-alueet. Viitattu 19.9.2015.
<http://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/>

EUR-lex. 2003. Mikroyritysten sekä pienten ja keskisuurten yritysten määritelmä. Sähköinen asiakirja versio. Viitattu 15.10.2015.
<http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=URISERV:n26026>

ISO 31000. 2015. ISO 31000 Riskienhallinta. Suomen Standardisoimisliitto SFS Ry. Viitattu 23.8.2015.
http://www.sfs.fi/julkaisut_ja_palvelut/tuotteet_valokeilassa/iso_31000_riskienhallinta

Kesäläinen, M. 2010. Kansallisen turvallisuusauditointikriteeristön (KATAKRI) suositusosuuden käyttöohje. Yritysturvallisuus EK Oy. Viitattu pdf-tiedostosta 30.10.2015.
http://www.ek.fi/ytnk08/fi/julkaisut_liitteet/KATAKRI_suositusohje_lopullinen.pdf

Koppa. 2015. Empiirinen tutkimus. Jyväskylän yliopiston menetelmäpolkuja humanisteille. Verkkosivut. Viitattu 24.9.2015.
<https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/empiirinen-tutkimus>

Koppa. 2015. Aineiston hankintamenetelmät. Jyväskylän yliopiston menetelmäpolkuja humanisteille. Verkkosivut. Viitattu 24.9.2015.
<https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/aineistonhankintamenetelmät>

Kunttu, T. 2009. Turvallisuusjohtamisjärjestelmien vertailu. Tutkimusraportti. Kymenlaakson ammattikorkeakoulu. Viitattu 24.9.2015.
http://www.merikotka.fi/metku/WP3_Turvallisuusjohtamisjarjestelmien_vertailu_f.pdf

Kurkela, R. 2015. Tilastokeskus. Tilastollinen tiedonkeruu -verkko-oppimateriaali. Verkko-opas on tuotettu Tilastokeskuksen ja Helsingin ammattikorkeakoulu Stadian yhteistyössä. Verkko-opas. Viitattu 18.9.2015. <https://www.stat.fi/virsta/tkeruu/>

Riskin arviointi. 2013. Työsuojeluhallinto. Verkojulkaisu. Tampere. Viitattu 15.9.2015.
http://www.tyosuojelujulkaisut.wshop.fi/documents/2013/11/Riskinarviointi_TSO14_2013.pdf

Suomen Standardisoimisliitto SFS Ry. 2013. SFS-EN ISO 19011 Johtamisjärjestelmän auditointiohjeet. Viitattu 23.8.2015.
<http://sales.sfs.fi/sfs/servlets/ProductServlet?action=productInfo&productID=248581>

SFS ry. 2015. Suomen Standardisoimisliitto SFS ry:n verkkosivu. Viitattu 24.9.2015.
http://www.sfs.fi/ajankohtaista/tapahtumakalenteri/uudistettu_sfs-en_iso_19011_tutuksi

SFS-tiedotus. 2014. Suomen Standardisoimisliitto SFS ry:n asiantuntijalehti. Suomen Standardisoimisliitto SFS ry. 5-2014. 46 vuosikerta 1/2014. Viitattu 10.9.2015.
http://www.sfs.fi/files/7835/5_2014_SFS_Tiedotus_opti.pdf

Taana, A. 2014. Määrällisen aineiston kerääminen. Pdf-tiedosto. Viitattu 14.9.2015.
<http://myy.haaga-helia.fi/-taaak/t/suunnittelu.pdf>

Ulkoministeriö. 2011. Kansallinen turvallisuusviranomaisen - Turvallisuusviranomaisten käsikirja yrityksille.
<http://formin.finland.fi/public/download.aspx?ID=89013&GUID=%7B1787C81D-6598-4469-AA23-FFB2A9DBC413%7D>

Kuviot

Kuvio 1: Aktiiviset ja piilevät virheet onnettomuuksien syntymisessä (Levä 2003, 19)	15
Kuvio 2: Rasmussenin sosio-tekninen onnettomuusketjun järjestelmämalli (Levä 2003, 22)	17
Kuvio 3: Riskienarvioinnin vaiheet, yksinkertaistettu kehämalli (Riskin arviointi 2013, 10)	19
Kuvio 4: Riskienhallinnan osa-alueet (Riskin arviointi 2013, 6).....	20
Kuvio 5: Turvallisuusjohtamisen osa-alueet (Elinkeinoelämän keskusliitto)	25
Kuvio 6: Katakrin mukaisen poikkeama-arvioinnin kokonaistulos	43
Kuvio 7: Turvallisuuden organisointi, poikkeamatilanteen tiedonkulku ja tilannekuvan ylläpito	52

Taulukot

Taulukko 1: Poikkeama-arvioinnin tulokset turvallisuuden eri osa-alueiden pääkysymysten mukaisesti eriteltynä jotka on esitetty puutteellisimmasta osa-alueesta lievimpään..... 43

Liitteet

Liite 1 Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100.....	76
Liite 2 Turvallisuuden vuotuinen toimintaohjelma, osa-alue A200	78
Liite 3 Turvallisuuden tavoitteiden määrittely, osa-alue A300	79
Liite 4 Riskien tunnistus, arviointi ja kontrollit, osa-alue A400	81
Liite 5 Turvallisuusorganisaatio ja vastuut, osa-alue A500	84
Liite 6 Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, osa-alue A600.....	86
Liite 7 Turvallisuusdokumentaatio ja sen hallinta, osa-alue A700	88
Liite 8 Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, osa-alue A800	89
Liite 9 Raportointi ja johdon katselmukset, osa-alue A900	91
Liite 10 KATAKRI III Hallinnollinen turvallisuus (T osa-alue)	92
Liite 11 Turvallisuuskyselyn vastaukset tulokset puutteellisuusjärjestyksessä	96

Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100

A100 (1/2)

<p>A 101.0</p> <p>Onko organisaation johto määrittänyt ja hyväksynyt turvallisuuspolitiikan? Onko politiikka tarkistettu määräajoin? <i>Kysymyksellä arvioidaan: Organisaation turvallisuusjohtamisen kypsyystasoa</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä dokumenttina tai osana yleisiä tavoitteita</p>	<p>TULOS & HAVAINNOT</p> <p>Johdon näkyvä hyväksyntä puuttuu. Ei ole yli kahteen vuoteen päivitetty ja päivämäärä puuttuu. Kaikki esimiehet eivät tunne turvallisuuspolitiikka termiä.</p>
<p>A 102.0</p> <p>Mitä turvallisuuden osatekijöitä turvallisuuspolitiikka ja/tai turvallisuuden johtaminen organisaatiossa kattaa? <i>Kysymyksellä arvioidaan: Turvallisuusjärjestelmän kokonaisvaltaisuutta ja järjestelmällisyyttä.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuuskirjasto sisältää ainakin tila-, tieto- ja henkilöstöturvallisuuden osa-alueet.</p>	<p>TULOS & HAVAINNOT</p> <p>Turvallisuusjohtamisessa ei riittävästi huomioida kokonaisvaltaisuutta, järjestelmällisyyttä ja säännöllistä vuosikello kiertoa. Ei huomioida riittävästi tietoturvasuutta, joka on merkittävä asia, koska se vaikuttaa myös toiminnan haavoittuvuuteen sekä jatkuvuudenhallintaan. Tietoturvasuosion puuttuu. Merkittävää, koska tehtävissä käsitellään sekä siltitutaan luottamukselliseen tietoon.</p>
<p>A 103.0</p> <p>Vastaako organisaation turvallisuuskirjasto toiminnan ja tuotteiden laajuutta ja toimintatapa ja niihin liittyviä turvallisuusriskejä?</p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on kirjattuna turvallisuutta koskevat perusasiat erillisenä projektidokumenttina tai osana yleisiä tavoitteita. Kysymyksellä arvioidaan: Turvallisuuspolitiikan tasoa.</p>	<p>TULOS & HAVAINNOT</p> <p>Otetaan huomioon pääasiat työkentelykohteissa ja kohteiden yleisimmät riski-, vaara- ja uhkatekijät. Toimialakohtaisesti dokumentaatiot keskittyvät työ-, henkilö- ja paloturvallisuuteen.</p>
<p>A 104.0</p> <p>Toimivatko organisaation kaikki tasot turvallisuuspolitiikan mukaisesti? <i>Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisältämien asioiden viemistä organisaation kaikille tasoille.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatio pystyy osoittamaan turvallisuusjärjestelmän turvallisuuspolitiikan tai projektidokumentin velvoitteiden valvonnan toteutumisen osana muuta valvontaa tai erillisenä turvallisuusauditointina</p>	<p>TULOS & HAVAINNOT</p> <p>Johdon näkyvät sitoutumiset (allekirjoitukset) puuttuvat. Johdon seuranta on osiltaan puutteellista. Yrityksen turvallisuutta valvotaan ja seurataan satunnaisesti (riippuu esimiehestä). Toiminnan turvallisuuspolitiikan mukaisuudesta ei voida olla varmoja, kun ei kattavasti seurata ja valvota.</p>
<p>A 105.0</p> <p>Huomioiko turvallisuuspolitiikka yleisen lainsäädännön ja paikallisten turvallisuusmääräysten sisältämät velvoitteet? <i>Kysymyksellä arvioidaan: Organisaatiota koskevan turvallisuuslainsäädännön tuntemusta ja lainsäädännön soveltamisen valvontaa.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa</p>	<p>TULOS & HAVAINNOT</p> <p>Mainittu osa, mutta ei kattavasti. Ei ole riittävästi avattu toimialakohtaisuutta ja lainsäädännön vaatimuksia. Huomioitu hyvin henkilö-, työ- ja palo- ja pelastusturvallisuuden osa-alueet. Lainsäädäntöä tunnetaan riittävästi. Ei olla kaikilta osin varmoja, koska ei tunneta laajuuden vaatimusta tai ei ole varmistavaa seurantamenettelyä. Nojaututaan liiaksi yhden henkilön seurannan ja valvonnan varaan. Henkilön riski, jos ei varajärjestelmää ja vastuunjako!</p>

Turvallisuuspolitiikka, turvallisuustoimintaa ohjaavat periaatteet ja määrittelyt, osa-alue A100

A100 (2 / 2)

A 105.1	Elinkeinoelämän suositukset:	TULOS & HAVAINNOT
<p>Pääkysymys: Onko toiminnan lakisääteiset vaatimukset huomioitu? (ex I 108.0)</p> <p><i>Lisäkysymykset: Miten lakisääteisiä vaatimuksia seurataan ja miten ne huomioidaan toiminnassa? Ovatko esimerkiksi henkilötietojen käsittelyn prosessit henkilötietolain edellyttämällä tasolla?</i></p> <p>Lähde lisätietoa ISO/IEC 27002 15.1, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietoa-aineiston käsittelyohje", VAHTI 8/2006, VAHTI 2/2010, http://www.finlex.fi/fi/laki/alkup/2004/20040588, http://www.finlex.fi/fi/laki/ajantasa/1999/19990621 http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/pdf/Tietoturvakartoitus_kysymyslista.pdf</p> <p>Käytännössä kaikkia organisaatioita koskee ainakin henkilötietolain (523/1999) 6§ ja sen asettamat vaatimukset henkilötietojen käsittelyn tarkoituksesta, henkilörekistereistä ja tietojen suojaamisesta koko tiedon elinkaaren ajalta sen kaikissa olomuodoissa. Vrt. turvaluokiteltujen aineistojen käsittelysäännöt</p>	<p>1) Toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty.</p> <p>2) Kansallisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansallisten käsittelysääntöjen, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.</p> <p>3) Kansainvälisten turvaluokiteltujen aineistojen luokittelu, jakelu ja käsittely toteutetaan kansainvälisten sopimusten, aineiston asettamien vaatimusten, ja/tai erillisen sopimuksen mukaisesti.</p>	<p>Koska ei tunneta laajuutta ja kaikkia vaatimuksia, ei esimiehistä myöskään varmista eikä valvo tai ylläpidä seurantamenettelyä.</p> <p>Käsittelyprosesseissa voi ilmetä väärää menettelytapoja ja riskejä, joita ei henkilörekistereihin pää-synhallinnassa ole huomioitu ja käsiteltyä ei ole ohjeistettu.</p> <p>Tietoa-aineistoja ei luokitella, eikä siten kaikkia käsiteltyä toteuteta edellytetyillä tavoilla.</p>
<p>A 106.0</p> <p>Pääkysymys: Onko turvallisuuspolitiikan sisältö tiedotettu kaikille työntekijöille, jotta heillä on selvä kuva omista turvallisuuteen liittyvistä velvollisuuksistaan ja vastuistaan?</p> <p><i>Lisäkysymys: Onko turvallisuuspolitiikkadokumentaatio jatkuvasti kaikkien saatavilla?</i></p> <p><i>Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisällön viemistä organisaation kaikille tasoille ja politiikan vaatimusten mukaisen toiminnan varmistamista jokapäiväisessä työssä.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuuspolitiikka tai vastaava turvallisuusohjeistus on koulutettu koko henkilöstölle ja se on helposti kerrattavissa esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla</p>	<p>TULOS & HAVAINNOT</p> <p>Kuuluu perehdytysohjelmaan ja se on löydettävissä intrasta</p> <p>Parannettavaa toteutuksen varmistamisessa ja tasossa, seuranta myös ontuu pahasti.</p> <p>Täysi varmuus puuttuu, riippuu perehdyttäjästä, myös seuranta ja valvonta on usein reaktiivista.</p> <p>Ei varmisteta, että jokainen työntekijä saa tiedon, sillä esimiehet viestivät kohteissa vaihtelevasti.</p>
<p>A 107.0</p> <p>Sisältääkö organisaation turvallisuuspolitiikka vaatimuksen kaikkien työntekijöiden sitoutumisesta jatkuvaan turvallisuustilanteen parantamiseen?</p> <p><i>Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisällön kattavuutta.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuuspolitiikka ja/tai -ohjeisto sisältää henkilökohtaisen sitoutumisen merkityksen.</p>	<p>TULOS & HAVAINNOT</p> <p>Täysi varmuus puuttuu, ei tarkisteta määräajoin, koska seuranta ja valvonta on usein vain reaktiivista.</p>
<p>A 108.0</p> <p>Onko turvallisuuspolitiikassa määritetty organisaation keskeiset turvallisuustavoitteet?</p> <p><i>Kysymyksellä arvioidaan: Turvallisuuspolitiikan sisällön kattavuutta.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Keskeiset tavoitteet on kuvattu turvallisuuspolitiikassa tai -ohjeistossa.</p>	<p>TULOS & HAVAINNOT</p> <p>Mainitaan johdon tuloskortti, jota kuitenkin ei ole olemassa. On huomioitu ainoastaan kohteiden riskit. Yritykselle ja liiketoiminnalle tärkeät suojattavat kohteet on määrittelemättä.</p>

Turvallisuuden vuotuinen toimintaohjelma, osa-alue A200

<p>A 201.0</p> <p>Onko organisaatiolla kirjoitettu ja dokumentoitu toimintaohjelma turvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?</p> <p><i>Kysymyksellä arvioidaan: Organisaation kykyä tunnistaa turvallisuuden kokonaisuus, oman toiminnan vahvuudet ja sellaiset alueet, joissa tarvitaan parantamista.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on toimintaohjelma, joka kattaa turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisaalueet. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.</p>	<p>TULOS & HAVAINNOT</p> <p>Toimintaohjelma huomioi ainoastaan työ- sekä henkilö- ja paloturvallisuuden, muu turvallisuuden osa-alueet jää takalalle.</p>
<p>A 202.0</p> <p>Onko toimintaohjelmassa eritelty menetelmät, vastuut ja aikataulut tavoitteiden saavuttamiseksi?</p> <p><i>Kysymyksellä arvioidaan: Ohjelman yksityiskohtaisuutta.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on turvallisuuden toimintaohjelma, jossa on kuvattu ainakin turvallisuusjohtamisen, henkilöstö-, tieto- ja tilaturvallisuuden kehittämisaalueiden osalta vaadittavat tavoitteet, vastuut ja aikataulut. Toimintaohjelma on erillinen dokumentti tai osa organisaation toimintasuunnitelmaa.</p>	<p>TULOS & HAVAINNOT</p> <p>Työsuojelutoimikunta toimiessaan kuvaa tavoitteita, (organisaation) vastuuta, toimenpiteitä ja aikatauluja vuosisuunnitelmasaan. Yrityksen turvallisuuden toimintaohjelma kattaa ainoastaan työ- ja henkilöstö-turvallisuuden osa-alueet.</p>
<p>A 203.0</p> <p>Tarkistetaanko toimintaohjelma säännöllisesti? Kysymyksellä arvioidaan: Ottaako organisaatio huomioon mahdollisesti muuttuvat tilanteet ja päivitetäänkö vuotuinen toimintaohjelma tarvittaessa</p>	<p>Elinkeinoelämän suositukset:</p> <p>Ohjelman tarkistaminen on osa jatkuvaa johtamiskäytäntöä.</p>	<p>TULOS & HAVAINNOT</p> <p>Työsuojelutoimikunta seuraa tavoiteohjelman edistymistä, josta myös raportoidaan.</p>
<p>A 204.0</p> <p>Onko organisaatiolla dokumentoitu ohjelma tietoturvallisuuden johtamiseksi ja turvallisuustyön tavoitteiden saavuttamiseksi?</p> <p>(ex I 102.0)</p> <p>Lähde/lisätieto</p> <p>PCI DSS 12.2, COBIT4.1 PO, COBIT 4.1 DSS, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschtz/guidelines/guidelines_pdf.p</p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on tietoturvasuunnitelma, toimintaohje, tai vastaava, ja siihen liittyvät ohjeet tarpeen mukaan.</p> <p>Suosittelaaan, että</p> <ol style="list-style-type: none"> 1) suunnitelma sisältää kuvaukset ainakin hallinnollisesta, fyysisestä ja tietoteknisestä tietoturvallisuudesta; 2) suunnitelma ottaa huomioon mahdollisen toimintaa säätelevän lainsäädännön (ml. tietosuoja); 3) suunnitelmaan liittyvät ohjeet ovat riittäviä suhteessa organisaatioon ja suojattavaan kohteeseen. 	<p>TULOS & HAVAINNOT</p> <p>Auditoinnissa ei ilmennyt havaintoja tai tietoa vaadituista suunnitelmallisesta toiminnasta tai dokumentaatioiden olemassaolosta.</p> <p>HRBookissa esitetyt tietosuoja ja tietoturva-asiat perehdytetty.</p> <p>HRBookissa esitetyt tietosuojaan ja tietoturvaan liittyvä ohjeistus on velvoittava, muttei riittävän laaja tai yksityiskohtainen kaikkiin käytössä oleviin laitteisiin ja tilanteisiin nähden.</p> <p>Auditoinnissa ei ilmennyt havaintoja tai tietoa vaadituista dokumentaatioista ja puuttuu tietoturvasuunnitelma.</p> <p>Ei ilmennyt vaadittuja käyttöoikeuksien hallinnasta, myöntämisvaltuuksista, menetelmistä tai pääsynhallintapolitiikasta dokumentaatiota valvontaa tai seuranta.</p> <p>Jotain mainintoja, mutta ei ole tehty tietoturvanäkökulmasta.</p>

Turvallisuuden tavoitteiden määrittely, osa-alue A300

A300 (1/2)

<p>A 301.0 Onko organisaation liiketoiminta ja sitä tukeva turvallisuuspolitiikka ja -ohjelma perusteena turvallisuusuyön tavoitteita asettaessa?</p> <p><i>Kysymyksellä arvioidaan: Muodostavatko politiikka, ohjelma ja tavoitteiden asettaminen kokonaisuuden.</i></p>	<p>Elinkeinoelämän suositukset: Turvallisuusuyön tavoitteet on asetettu politiikan mukaisesti, selkeästi ja mitattavasti.</p>	<p>TULOS & HAVAINNOT Johdon tuloskorttia ei käytetä, tavoitteita ei aseteta realistisesti mitattaviksi, joita ei myöskään mittareilla seurata. Tavoitteita asetetaan työturvallisuusasioloissa.</p> <p>Ainoastaan työ-, henkilöstö- ja paloturvallisuudessa asetetaan tavoitteita. Johdon tuki ja hyväksyntä puuttuvat ja turvallisuusuyöiminta tapahtuu työturvallisuuden näkökulmasta.</p>
<p>A 302.0 Onko organisaatio asettanut turvallisuustavoitteet organisaation eri hierarkiatasolle ja/tai toiminnolle?</p> <p><i>Kysymyksellä arvioidaan: Tavoitteiden konkreettista asettamista ja eri osatavoitteiden merkityksellisyden ymmärtämistä organisaation eri osien ja hierarkiatasojen osalta. Tavoitteiden dokumentoinnilla varmistetaan se, että vaatimustasoa voidaan kehittää jatkuvan parantamisen periaatteella.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatiolla on selkeät ja dokumentoidut turvallisuustavoitteet, jotka kattavat ohjelman mukaiset turvallisuuden osa-alueet ja eriteltyä organisaation toiminnassa tarvittavat osat ja tasot.</p>	<p>TULOS & HAVAINNOT Ainoastaan työ-, henkilöstö- ja paloturvallisuudessa asetetaan tavoitteita, koska suurin osa tapahtuu asiakkaan tiloissa ja turvallisuusuyössä.</p> <p>Ainoastaan työ-, henkilöstö- ja paloturvallisuudessa asetetaan jotain dokumentoituja tavoitteita.</p>
<p>A 303.0 Onko tavoitteet asetettu siten, että niiden saavuttaminen on mitattavissa?</p> <p><i>Kysymyksellä arvioidaan: Tavoitteiden konkreettista ja realistista asettamista sekä laadullisten mittareiden sisällyttämistä tavoitteisiin.</i></p>	<p>Elinkeinoelämän suositukset: Turvallisuusuyöiminnan tavoitteet on asetettu konkreettisesti ja mitattavasti.</p>	<p>TULOS & HAVAINNOT Johdon tuloskorttia ei käytetä, tavoitteita ei aseteta realistisesti mitattaviksi, joita ei myöskään mittareilla seurata. Tavoitteita asetetaan työturvallisuusasioloissa.</p>
<p>A 304.0 Onko tavoitteiden saavuttamiselle asetettu aikataulu?</p> <p><i>Kysymyksellä arvioidaan: Tavoitteiden konkreettista ja realistista asettamista.</i></p>	<p>Elinkeinoelämän suositukset: Tavoitteiden saavuttamiselle on asetettu aikataulu.</p>	<p>TULOS & HAVAINNOT Ei aseteta realistisia aikatauluja tavoitteille, koska vatuut, aikataulut jne. puuttuvat samoin seuranta, on ainoastaan palaverimuistioita.</p>

Turvallisuuden tavoitteiden määrittely, osa-alue A300

A300 (2 / 2)

<p>A 305.0</p> <p>Onko seuraavat tekijät otettu huomioon tavoitteiden asettamisen yhteydessä:</p> <p>a. tunnistetut riskit</p> <p>b. organisaation oman toiminnan ja/tai liiketoiminnan vaatimukset</p> <p>c. tekniset vaatimukset ja mahdollisuudet</p> <p>d. taloudelliset vaatimukset</p> <p>e. muiden intressiryhmien vaatimukset (esim. asiakkaat, viranomaiset)</p> <p>f. lainsäädännön ja/tai muiden ohjeistojen sekä sopimusten vaatimukset</p> <p><i>Kysymyksellä arvioidaan: Onko tavoitteita asetettaessa tunnistettu mm. edellä kuvatut vaatimukset, mahdollisuudet ja rajoittavat tekijät</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Asetettavat tavoitteet sisältävät tarvittavilta osin kuvauksen liittymisestä tunnistettuihin riskeihin, teknisiin ja taloudellisiin vaatimuksiin sekä mahdollisuuksiin, organisaation oman toiminnan ja/tai liiketoiminnan vaatimuksiin, muiden intressiryhmien vaatimuksiin ja/tai lainsäädännön/muiden ohjeistojen vaatimuksiin huomioiden tekijät a), b), c), d), e), f).</p>	<p>TULOS & HAVAINNOT</p> <p>Osittain kohteiden mukaisesti riskit on kartoitettu.</p> <p>Ei ole käytössä varmistusmenetelyä, ei voida olla täysin varmoja?</p> <p>Tietoteknisiä mahdollisuuksia ei ole huomioitu riittävästi, kun ei ole riittävästi ICT-asiantuntemusta käytettävissä?</p> <p>Ad-Hoc tarpeiden ja tilanteiden mukaisesti toimimalla, muttai täyttä varmuutta riittävydestä.</p>
<p>A 306.0</p> <p>Onko koko suojattavan tiedon käsittely-ympäristö suojattu organisaation tietoturvaperiaatteiden ja tiedon merkityksen/</p> <p><i>Lisäkysymykset: Kattavatko suojaukset kaikki loogisesti kytketyt tietoverkot ja -järjestelmät, joissa suojattavaa tietoa käsitellään? Kattavatko suojaukset myös sellaiset tietoverkot ja -järjestelmät, joihin tietoa viedään tai joista tietoa tuodaan ilmaan yli esimerkiksi USB -muisteilla?</i></p> <p>Lähde/lisätieto</p> <p>Kansallisen turvallisuusviranomaisen ”Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje”, VAHTI 2/2010, VAHTI 3/2010</p> <p>Vaatimuksen päätavoitteena on varmistua siitä, että koko suojattavan tiedon käsittely ympäristö tulee suojatuksi asianmukaisesti, ja että esimerkiksi pääjärjestelmään kytketyt apujärjestelmän kautta ei ole luvattonta pääsyä suojattavaan tietoon. Oheistavoitteena on varmistua siitä, että suojattavaan tietoon ei ole luvattonta pääsyä esimerkiksi heikosti suojatun tilapäis-, kokeilu-, tai luvattomasti asennetun verkon kautta.</p> <p>Erityisesti turvaluokitellun aineiston tapauksessa tulee koko suojattavan tiedon käsittely ympäristön olla suojattu ja hyväksytty käsiteltävän tiedon turvaluokan mukaisesti. Vaatimus kattaa mm. kaikki verkkoon/järjestelmään kytketyt muut verkot/järjestelmät sekä kaikki käsittely-ympäristöt, joihin turvaluokiteltua</p>	<p>Elinkeinoelämän suositukset:</p> <p>Kaikki suojattavaa tietoa käsittelevät tietoverkot ja -järjestelmät ovat organisaation tietoturvaperiaatteiden mukaisesti suojattuja.</p>	<p>TULOS & HAVAINNOT</p> <p>Ei dokumentaatiota.</p> <p>Turvaluokitusta ei ole käytössä eikä asiakirjoja merkittä tai suojata.</p> <p>Ei voida varmistaa, että on suojattu, kun on ulkoistettu palvelu, jota ei ole auditoitu jätettävä.</p> <p>Turvaluokitettua aineistolle ja asiakirjoille ei ole laadittu ohjeistusta suojaus- tai luokitusmerkinnästä eikä käsittelyohjeita ole käytössä.</p>

Riskien tunnistus, arviointi ja kontrollit, osa-alue A400

A400 (1/3)

<p>A 401.0</p> <p>Onko organisaatiolla menetelmät tunnistaa ja arvioida turvallisuusriskit?</p> <p><i>Kysymyksellä arvioidaan: Priorisoiko organisaatio turvallisuustyönsä arvioimalla riskit.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatio arvioi turvallisuuden kokonaisuuteen liittyvät riskit ja riskienarviointi on turvallisuustyön tärkeysjärjestyksen peruste. Menettelytapa on säännöllinen ja tulokset dokumentoidaan.</p>	<p>TULOS & HAVAINNOT</p> <p>Riskienarvioita tehdään kohteissa työturvallisuuden näkökulmasta, joka on myös lähtökohtana turvallisuustyölle. Riskienhallinta-prosessin puuttuessa ei voida todeta näin tapahtuneen.</p> <p>Ei havaittu riskienarviointien tekemistä tai vuosittaisia päivitysten säännönmukaisuutta. Tehdyt arvioinnit kohteista dokumentoitu.</p>
<p>A 401.1</p> <p>Pääkysymys: Onko toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät, prosessit) tunnistettu?</p> <p>(ex I 103.0)</p> <p><i>Lisäkysymykset: Mitä uhkia niihin kohdistuu? Onko suojattaville kohteille määritetty vastuuhenkilöt?</i></p> <p>Lähde/lisätieto a</p> <p>ISO/IEC 27002 7.1, COBIT 4.1 PO9, VAHTI 8/2006.</p>	<p>Elinkeinoelämän suositukset:</p> <ol style="list-style-type: none"> 1) Suojattavat kohteet (assets) on tunnistettu. 2) Suojattaviin kohteisiin kohdistuvat uhat on tunnistettu. 3) Suojattaville kohteille on nimetty omistaja/vastuuhenkilö. 4) Suojattavien kohteiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (vrt. A 401.2). 	<p>TULOS & HAVAINNOT</p> <p>Uhkien tunnistus kohdistuu henkilö- ja työturvallisuuden suojauksiin sekä as.kohteisiin ja kohteesta vastaa kohde-esimies. Yrityksen toiminnalle tärkeitä suojattavia kohteita eikä riskejä ole tunnistettu tai määritelty.</p>
<p>A 401.2</p> <p>Miten suojattaviin kohteisiin kohdistuvia riskejä arvioidaan?</p> <p>(ex I104.0)</p> <p>Lähde/lisätieto a</p> <p>ISO/IEC 27001 luku 4, ISO/IEC 27002 7.1, COBIT 4.1 PO9, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokittelun tietoaineiston käsittelyohje", VAHTI 8/2006, VAHTI 2/2010:n liite 5 (TTT), EU:n turvallisuussäädösten 6952/2/11 REV2 /1.4.2011 5. artikla.</p>	<p>Elinkeinoelämän suositukset:</p> <ol style="list-style-type: none"> 1) Suojattaviin kohteisiin (vrt. A 401.1) kohdistuvia riskejä arvioidaan jollain järjestelmällisellä menetelmällä. 2) Arviointi tapahtuu vähintään vuosittain ja lisäksi merkittävien muutosten yhteydessä. 3) Valitut suojausmenetelmät on asianmukaisesti suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin. 4) Johto on hyväksynyt valitut suojausmenetelmät ja jäännösriskit 	<p>TULOS & HAVAINNOT</p> <p>Kohde-esimies tekee kohteesta oman riskiarvion. Arvioinnissa ei käytetä järjestelmällistä tai vakioitua kartoitusmenetelmää.</p> <p>Kokonaisarviointia ei tehdä suostetusti, ainoastaan työsuojelu-toimikunnan toiminnan puitteissa.</p> <p>Työsuojelutoimikunta käsittelee suojaustoimintojen asianmukaisuutta työturvallisuusasioissa. Ei dokumentoitua suojaustoimien päätös tai hyväksymis asiakirjoja.</p> <p>Johtoryhmään kuuluva turvallisuudesta vastaava hyväksyy suojaustoimet.</p>
<p>A 402.0</p> <p>Kattavatko nämä menetelmät normaalin toiminnan, erityistilanteet, onnettomuudet ja hätätapaukset? Otetaanko alirakoitsijat ja palveluntarjoajat huomioon?</p> <p><i>Kysymyksellä arvioidaan: Riskienarvioinnin kattavuutta.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Riskienarviointi kattaa ainakin turvallisuusjohtamisen sekä henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Asiat on huomioitu tarvittavien sidosryhmien osalta.</p>	<p>TULOS & HAVAINNOT</p> <p>Riskienarviointimenetelmä ei huomioi erityistilanteita, mutta hätätapauksia jonkin verran jolloin arviot perustuvat ainoastaan kohteen työturvallisuuteen vaikuttaviin tekijöihin.</p> <p>Riskien arviointi tapahtuu kohteessa ja siihen liittyviin sidosryhmiin. Riskienarviointi ei huomioi tietoturvallisuuden osa-aluetta eikä ulkoistettua IT-palveluntuottajaa.</p>

Riskien tunnistus, arviointi ja kontrollit, osa-alue A400

A400 (2/3)

<p>A 403.0 Dokumentoidaanko riskienarviointien tulokset ja päivitetäänkö ne säännöllisesti?</p> <p><i>Kysymyksellä arvioidaan: Onko organisaatiossa todennettava järjestelmä riskien arvioinneista tallenteineen.</i></p>	<p>Elinkeinoelämän suositukset: Riskienarviointi tehdään vähintään vuosittain ja organisaation tilanteen muuttuessa siten, että on tarkoituksen mukaista päivittää tehty arvio. Riskien arvioinnit dokumentoidaan siten, että ne ovat todennettavissa.</p>	<p>TULOS & HAVAINNOT Ei havaittu riskienarviointien tekemistä tai vuosittaista päivitysten säännönmukaisuutta. Tehdyt arvioinnit kohteista dokumentoitu.</p> <p>Kohdekansioon liitetään kohteesta tehty riskienarviointilomake.</p>
<p>A 404.0 Otetaanko riskienarviointien havainnot huomioon turvallisuustoiminnan tavoitteita asetettaessa?</p> <p><i>Kysymyksellä arvioidaan: Onko riskienarviointi osa laadukasta turvallisuustoimintaa, joka tähtää jatkuvaan toiminnan tason parantamiseen.</i></p>	<p>Elinkeinoelämän suositukset: Riskienarvioinnin tulokset on huomioitu turvallisuustoiminnan tavoitteita asetettaessa.</p>	<p>TULOS & HAVAINNOT Työturvallisuusasioissa työsuojelutoimikunta huomioi riskiarvioinneissa tehtyjä havaintoja tavoitteita asettaessa. Kattaa vain henkilö-, tila- ja työturvallisuusasiat.</p>
<p>A 405.0 Voidaanko riskienarvioinnin tulosten perusteella priorisoida riskit?</p> <p><i>Kysymyksellä arvioidaan: Saadaanko tuloksena perusteet riskienhallinnan toimenpiteiden valinnalle, tärkeysjärjestykselle ja kiireellisyydelle.</i></p>	<p>Elinkeinoelämän suositukset: Riskienarvioinnin tuloksena riskit luokitellaan tärkeysjärjestykseen.</p>	<p>TULOS & HAVAINNOT Dokumentoitu kokonaisriskiarvioinneista tehtyjä luokituksia, priorisointia sekä vaikuttavuusarvioiteja ei ole havaittu tehdyn.</p>
<p>A 406.0 Antavatko riskienarvioinnit perusteet turvallisuuskoulutuksen vaatimuksille?</p> <p><i>Kysymyksellä arvioidaan: Onko riskienarviointi myös työkalu, joka tukee koulutuksen suunnittelua yhtenä keinona pienentää riskin vaikutusta.</i></p>	<p>Elinkeinoelämän suositukset: Riskienarviointien tulokset vaikuttavat suunnitellun koulutuksen sisältöön. Koulutus tunnustetaan yhtenä keinona vaikuttaa riskien hallintaan.</p>	<p>TULOS & HAVAINNOT Yrityksessä on juuri toteutettu laaja konsepti- ja turvallisuus-koulutus. Tuloksena työ-turvallisuuden parantuminen.</p>
<p>A 407.0 Onko organisaatiolla menetelmät valvoa turvallisuuden riskienarviointien perusteella tehtyjen toimenpiteiden toteuttamista ja tehokkuutta?</p> <p><i>Kysymyksellä arvioidaan: Toteutuuko riskienarvioinnin perusteella valittujen toimenpiteiden haluttu vaikutus.</i></p>	<p>Elinkeinoelämän suositukset: Turvallisuusjohtamisen prosessi sisältää riskienarvioinnin perusteella tehtyjen toimenpiteiden toteuttamisen ja tehokkuuden arvioinnin.</p>	<p>TULOS & HAVAINNOT Tehokkuusarviointia ei ole toteutettu eikä analysoitu toteutettujen toimenpiteiden vaikuttavuutta. Suojaustoimien toteutuksen tehokkuutta ja vaikutuksia ei seurata, arvioida eikä tuloksia dokumentoida, kuin työturvallisuuden osa-alueessa.</p>

Riskien tunnistus, arviointi ja kontrollit, osa-alue A400

A400 (3 / 3)

A 408.0	Elinkeinoelämän suositukset:	TULOS & HAVAINNOT
<p>Pääkysymys: Miten organisaation tietoturvaluottuutta arvioidaan?</p> <p><i>Lisäkysymys: Kehitetäänkö toimintaa havaintojen perusteella?</i> (ex I 105.0)</p> <p>Lähde/lisätietoa ISO/IEC 27002 6.1.8, ISO/IEC 27004, VAHTI 8/2006, Vaatimusten täytyminen voidaan todentaa pyytämällä esimerkkejä siitä, miten tietoturvaluottuutta on seurattu, arvioitu ja kehitetty.</p>	<p>Organisaation tietoturvaluottuuden toimintamallia ja tietoturvaluottuuden käytännön toteuttamista seurataan, arvioidaan ja kehitetään jatkuvasti.</p>	<p>Ei havaittu toteutuksia tietoturvaluottuuskäytänteiden noudattamisen seurannasta, arvioinnista eikä jatkuvasta kehittämistä.</p>
<p>A 409.0</p> <p>Miten tietoturvaluottuudesta on huolehdittu alihankinta-, palveluhankinta- ja muussa vastaavassa yhteistyössä? (ex I 106.0)</p> <p><i>Huom! Osa kansainvälisistä aineistoista ei saa luovuttaa alihankkijoille ja vastaaville tilan viranomaisen etukäteissuostumusta edes suojaustasolla IV. Tämä on varmistettava tapauskohtaisesti.</i></p> <p>ISO/IEC 27002 6.2.1, ISO/IEC 27002 6.2.2, ISO/IEC 27002 10.6.1, ISO/IEC 27002 12.1.1, COBIT 4.1 A15, COBIT 4.1 DS1, COBIT 4.1 DS2, Kansallisen turvaluottuussuostumuksen ”Kansainvälisen turvaluottuussuostumuksen käsittelyohje”, VAHTI 8/2006, EU:n turvaluottuussäännöstö 6952/2/11 REV2 /1.4.2011 11. artkla, EU:n turvaluottuussäännöstö 6952/2/11 REV2 /1.4.2011 liite V.</p> <p>Lähde/lisätietoa</p> <p>Huolehdittava myös salassapitosuostumukset (P 407.0). Alihankkijoilta ja vastaavilta voidaan tapauskohtaisesti vaatia myös säännölliset raportit tietoturvaluottuuden nykytilasta (esim. kuukauden havainnot, hyökkäysyritykset, poikkeukset, jne.).</p>	<p>Elinkeinoelämän suositukset:</p> <ol style="list-style-type: none"> 1) Tarjouspyyntöihin on liitetty tietoturvaluottuuskäytännöt. 2) Ulkopuolisiin tahoihin (esim. ulkoistuskumppaneihin) liittyvät riskit on tunnistettu ja asianmukaiset turvamekanismit toteutettu. 3) Palveluihin on määritelty palvelun laatu (SLA). 4) Ulkoistettujen tietojenkäsittelypalveluiden toimittajien kanssa on sovitettu menettelytavat tietoturvaluottuuskäytännön varalle. 	<p>TULOS & HAVAINNOT</p> <p>Ei havaittu toteutettua tietoturvaluottuuskäytännön liittämissä tarjouspyyntöihin.</p> <p>Palveluntuottajien riskien tunnistamisesta ja turvamekanismeista ei löytenyt viitteitä.</p> <p>Ei havaittu palveluntuottajille määritetyistä laatu (SLA), eikä tietoturvaluottuuskäytännön varalle sovitusta toiminta- ja menettelytapoista.</p> <p>Ei ole sovitettu mitään palveluntuottajan kanssa toiminta- ja menettelytapoista tietoturvaluottuuskäytännön varalle.</p> <p>Ei havaittu tehdyn salassapitosuostumusta ulkopuolisten palveluntuottajien kanssa.</p> <p>Ei tehty suostumusta palveluntuottajan säännöllisestä tietoturvaluottuuden tilan raportoinnista.</p>
<p>A 410.0</p> <p>Miten organisaatiossa toimitaan tietoturvaluottuuskäytännöissä?</p> <p><i>Lisäkysymys: Miten tietoturvaluottuuskäytännön hallinta on käytännössä toteutettu?</i> (ex I 107.0)</p> <p>Lähde/lisätietoa ISO/IEC 27002 13.2.1, PCIDSS 12.9, COBIT 4.1 DS8, VAHTI 3/2010, EU:n turvaluottuussäännöstö 6952/2/11 REV2 /1.4.2011 13. artkla, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/guidelines/guidelines.pdf</p> <p>Vrt. I 408.0. Taho, jolle poikkeamat raportoidaan, riippuu tiedon omistajasta. Taho voi olla esimerkiksi NCSA-FI, CERT-FI, puolustusvoimien taho tai Euroopan Unionin neuvoston CERT-toimija.</p>	<p>Elinkeinoelämän suositukset:</p> <p>Tietoturvaluottuuskäytännön hallinta on</p> <ol style="list-style-type: none"> 1) suunniteltu, 2) ohjeistettu/ koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, ja erityisesti 4) viestintäkäytännöt ja -vastuut on sovitettu. 	<p>TULOS & HAVAINNOT</p> <p>Ei suunniteltu tietoturvaluottuuskäytännön hallintaprosesseja.</p> <p>Ei ole ohjeistettu / koulutettu tietoturvaluottuuskäytännön hallintaa ei ole dokumentoitu. Tietoturvaluottuuskäytännön ei ole eriytetty muusta poikkeamatiedosta.</p> <p>Ei ole sovitettu tietoturvaluottuuskäytännön viestintäkäytännöstä ja vastuista.</p> <p>Ilmoitusten perillemenosta ei ole täyttä varmuutta, eikä sitä tehdäänkö kaikista tietoturvaluottuuskäytännön ilmoitusta.</p> <p>Ei ole sovitettu palveluntuottajien kanssa toiminta- ja menettelytapoista tietoturvaluottuuskäytännön varalle.</p>

Turvallisuusorganisaatio ja vastuut, osa-alue A500

A500 (1/2)

<p>A 501.0</p> <p>Ovatko turvallisuusjärjestelmän vastuut määritetty? Kattavatko määritetyt organisaation eri tasot?</p> <p><i>Kysymyksellä arvioidaan: Ovatko turvallisuusjärjestelmän vastuut asetetut siten, että kaikki toiminnot ja organisaation tasot on katettu.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuusorganisaatio kattaa ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Vastuulliset henkilöt on nimetty.</p>	<p>TULOS & HAVAINNOT</p> <p>Työsuojelutoimikunta toimies-sään kuvaa tavoitteita, (organisaation) vastuuta, toimenpiteitä ja aikatauluja vuosisuunnitelmassaan. Yrityksen turvallisuuden toimintaohjelma kattaa ainoastaan työ- ja henkilöstö-turvallisuuden osa-alueet.</p> <p>Ainoastaan työ-, henkilöstö- ja paloturvallisuudessa asetetaan tavoitteita, koska suurin osa tapahtuu asiakkaan tiloissa ja turvallisuusjärjestelmässä.</p>
<p>A 501.1</p> <p>Onko organisaation tietoturvallisuudella johdon tuki?</p> <p>Miten tuki käytännössä näkyy organisaation toiminnassa?</p> <p>(ex I 101.0)</p> <p>Lähde/lisätietoja</p> <p>ISO/IEC 27002 5.1.1, 5.1.2, 6.1.1, 6.1.3, 7.1 ja 8.2.1, PCI DSS 12.1, 12.3.1, 12.4 ja 12.5, COBIT 4.1 PO4 ja PO6.</p> <p>https://www.bsi.bund.de/SharedDocs/Download/EN/BSI/Grundschatz/guidelines/guidelines.pdf</p> <p>Suosittelaa, että järjestelmille on määritetty ylläpitovastuun lisäksi myös omistajat. Suositellaan, että tekninen ylläpito ei ole sama kuin omistaja.</p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaation tietoturvallisuudella on johdon tuki.</p> <p>Suosittelaa vähintään, että</p> <p>1) tietoturvallisuus on vastuutettu (johdon vastuut, tietohallinnon / järjestelmien ylläpidon vastuut, peruskäyttäjän vastuut, jne.);</p> <p>2) organisaatiolla on johdon hyväksymät tietoturvaperiaatteet ja -käytännöt;</p> <p>3) tietoturvaperiaatteet ja -käytännöt on saatettu koko organisaation tietoon;</p> <p>4) tietoturvaperiaatteet ja -käytännöt katselmoidaan vuosittain ja aina, kun merkittäviä muutoksia tapahtuu;</p> <p>5) johto edellyttää, että työntekijät, toimittajat ja ulkopuoliset tietojen käsittelijät toimivat organisaation tietoturvaperiaatteiden mukaisesti;</p> <p>6) tietoturvallisuudelle on varattu toimintavälineisiin nähden riittävät resurssit.</p>	<p>TULOS & HAVAINNOT</p> <p>Yrityksellä ei ole julkaistu tietoturvapoliittikkaa, eikä tietoturvasuunnitelmaa, jonka johto voisi hyväksyä.</p> <p>Yrityksellä ei ole julkaistu tietoturvapoliittikkaa, eikä tietoturvasuunnitelmaa, jota johto voisi tukea.</p> <p>On vastuutettu sovelluksia työnkuvan mukaisesti, mutta ei dokumentoitu (omist-tjv +ylläpito) ja tietoturvan osaa ei ole korostettu.</p> <p>Peruskäyttäjien yleisvastuu perehdytetty ja HRBook-ohjeissa löytyy yleismainintoja.</p> <p>Tietoturvaa ei katselmoita vuosittain eikä muutoksissa oteta erikseen esille.</p> <p>Työntekijöitä edellytetään tietoturvaohjeiden noudattamista, mutta seuranta ja valvonta satunnaista tai puuttuu kokonaan.</p> <p>Tietohallinnon ja tietoturvan toteuttamiseksi ei ole riittäviä resursseja ja asiantuntemusta, vastuuhenkilöitä ei ole nimetty, vastuutettu eikä valtuuksia annettu.</p>
<p>A 502.0</p> <p>Ovatko roolit, vastuut ja toimeenpanovalta tiedotettu organisaatiossa ja niille ulkopuolisille tahoille, joiden on tunnettava turvallisuusorganisaation rakenne?</p> <p><i>Kysymyksellä arvioidaan: Tiedätkö organisaatio ne henkilöt, jotka vastaavat eri turvallisuuden osa-alueista ja jotka samalla pystyvät tukemaan eri ongelmatilanteissa.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuusorganisaatio on koulutettu henkilöstölle ja tieto on saatavissa päivitettyinä esimerkiksi tietojärjestelmän tai ilmoitustaulun avulla.</p>	<p>TULOS & HAVAINNOT</p> <p>On vain työturvallisuusorganisaatio, joka kokoontuu 3 krt./ vuodessa. Päivitetty tieto löytyy toimintaohjelmasta.</p> <p>Työturvallisuusorganisaatio, jossa turvallisuudesta vastaava toimii ja johdon roolit sekä vastuut on tiedotettu. Varamiesjärj. ei ole kaikille selvä ja puolet ei tiedä miten toimia ja keneltä saa apua.</p>

Turvallisuusorganisaatio ja vastuut, osa-alue A500

A500 (2/2)

A 503.0	Elinkeinoelämän suositukset:	TULOS & HAVAINNOT
<p>Onko turvallisuustyölle suunnattu riittävästi resursseja työn toteuttamiseksi, kontrolloimiseksi sekä parantamiseksi?</p> <p><i>Kysymyksellä arvioidaan: Onko turvallisuustyöllä realistiset onnistumisen mahdollisuudet.</i></p> <p style="text-align: right;">Resurssien tulisi kattaa: – henkilöstö ja erityisosaaminen – teknologiset ja taloudelliset resurssit</p>	<p>Turvallisuusjohtaminen kattaa mm.</p> <ol style="list-style-type: none"> 1) henkilöstön, 2) teknologian ja 3) taloudellisten resurssien riittävyyden arvioinnin. 	<p>Johdolle ja esimiehistöille ei ole annettu riittävästi resursseja turvallisuusjohtamis tehtävän suorittamiseksi, sillä ajan puutteen vuoksi turvallisuustyön toteutus, kontrollointi ja jatkuva parantaminen toteutuu parhaalla mahdollisella tavalla.</p>
<p>A 504.0</p> <p>Onko organisaation ylin johto määrittänyt henkilön, joka on vastuussa turvallisuustoiminnan kehittamisestä ja johtamisesta sekä siitä, että turvallisuustyö kattaa kaikkien organisaation tasojen tarpeet?</p> <p><i>Kysymyksellä arvioidaan: Onko turvallisuudesta vastaavalla henkilöllä johdon tuki ja aseman tuoma valtuus ja onko asetettu tehtävä riittävän laaja-alainen kokonaisuuden hallitsemiseksi. Tehtävä voi olla osa henkilön muuta toimenkuvaa.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on turvallisuudesta vastaava henkilö, jolla on riittävät mahdollisuudet johtaa turvallisuustoimintaa ja hallita ainakin henkilöstö-, tieto- ja tilaturvallisuuden osa-alueet. Tehtäväkenttä voi olla myös jaettu, mikäli se on organisaation toiminnan kannalta tarkoituksenmukaista</p>	<p>TULOS & HAVAINNOT</p> <p>Turvallisuusjohtamisessa ja -organisaatiossa ei riittävästi huomioida kokonaisvaltaisuutta, järjestelmällisyyttä ja säännöllistä vuosikello kiertoa. Ei huomioida riittävästi tietoturvallisuutta, joka on merkittävä asia, koska se vaikuttaa myös toiminnan haavoittuvuuteen sekä jatkuvuudenhallintaan.</p>
<p>A 505.0</p> <p>Onko nimetyllä turvallisuustyöstä vastaavalla henkilöllä vastuu ja valtuus sen varmistamiseksi, että turvallisuuden johtamisjärjestelmä on muodostettu niiden vaatimusten mukaisesti, joita tavoitteissa on asetettu?</p> <p><i>Kysymyksellä arvioidaan: Onko turvallisuustoimintaa johtavalla henkilöllä mahdollisuus vaikuttaa johtamisjärjestelmään siten, että turvallisuustavoitteiden saavuttaminen on mahdollista.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuudesta vastaava henkilö on organisaatiossa sellaisessa asemassa, että hänellä on mahdollisuus vaikuttaa turvallisuuden toteuttamiseen. Vaikuttamismahdollisuus on yksilöitävä organisaation prosessikuvauksessa ja/tai henkilön tehtäväkuvauksessa.</p>	<p>TULOS & HAVAINNOT</p> <p>Turvallisuudesta vastaavien vaikuttamismahdollisuuksia ei ole riittävästi yksilöity (mm. prosessikuvaukset / turvallisuusorganisaatiossa / henkilön toimenkuvauksessa).</p>
<p>A 506.0</p> <p>Onko organisaation johto sitoutunut turvallisuustavoitteisiin ja niiden saavuttamiseen sekä turvallisuuden jatkuvaan parantamiseen?</p> <p><i>Kysymyksellä arvioidaan: Toteutuuko turvallisuustyöhön sitoutuminen organisaation kaikilla tasoilla. Organisaation johdon esimerkin vaikutus on ratkaiseva tekijä.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaation johto on mukana turvallisuustyön tavoitteiden asettamisessa, menetelmien valinnassa ja tavoitteiden seurannan arvioinnissa.</p>	<p>TULOS & HAVAINNOT</p> <p>Johtoryhmä asettaa hyviä tavoitteita, mutta ei valita tai osoiteta menetelmiä, aikatauluja, vastuuta, vaatimuksia ja resursseja.</p>

Onnettomudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, A600

A600 (1/2)

<p>A 601.0 Onko organisaatiolla jatkuvuudenhallintamenettely? <i>Kysymyksellä arvioidaan: Onko organisaatio tunnistanut toimintaa uhkaavat häiriöt ja varautunut niistä sellaisiin, jotka voivat hidastaa tai estää päättävöiteiden saavuttamista.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatio on tunnistanut jatkuvuuttaan uhkaavat tärkeimmät seikat ja varautunut niihin suojaus-, varmennus-, kahdennus- yms. menettelyin. Organisaatiolla on lakisääteinen vakuutusurva.</p>	<p>TULOS & HAVAINNOT Yrityksessä ei ole jatkuvuussuunnittelua joilla varaudutaan erilaisiin suojaus-, varmennus-, kahdennus- yms. menettelyin.</p>
<p>A 602.0 Onko organisaatiossa määritetty onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien käsittelystä ja tutkinnasta vastaavat henkilöt? <i>Kysymyksellä arvioidaan: Onko organisaatio ottanut huomioon turvallisuuspoikkeamat ja onko niiden hallinta määritetty ja organisoitu. Onko yhteistoiminta viranomaisten suuntaan suunniteltu.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia.</p>	<p>TULOS & HAVAINNOT Määrittely ja työkuvaus sekä valtuudet puuttuvat, mutta turvallisuusvastaava toimii myös työturvallisuuspäällikkönä ja siten vastaa tutkimisesta sekä toimenpiteistä. Turvallisuusvastaavana toimiva henkilö toimii turvallisuuspoikkeamien tutkimisesta vastaavana henkilönä. Tietoturva- ja poikkeamista vastuullista ei ole nimetty.</p>
<p>A 603.0 Onko vastuut kriisitilanteiden, onnettomuuksien, vaaratilanteiden ja turvallisuuspoikkeamien vaikutusten ennalta pienentämiseksi määritetty? <i>Kysymyksellä arvioidaan: Onko organisaatio ottanut ennakoita huomioon poikkeavien tilanteiden ilmenemisen ja onko riskien pienentäminen määritetty ja organisoitu.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatio on määrittänyt poikkeamatilanteiden johtamisen osana turvallisuuden organisointia. Valtuudet ja vastuut on kuvattu henkilöiden tehtäväkuvauksissa.</p>	<p>TULOS & HAVAINNOT Vaikka turvallisuudesta vastaava on nimetty ei työntehtävissä ole riittäviä kuvauksia vastuista ja valtuuksista. Selkeiden työtehtäväkuvauksien puuttuessa (roolit, vastuut ja valtuudet) henkilöt eivät pysty toteuttamaan ennaltaehkäiseviä toimia tehokkaasti.</p>
<p>A 604.0 Onko organisaatiolla menetelmät turvallisuuspoikkeamien havaitsemiseksi ja suojaavien sekä korjaavien toimenpiteiden tekemiseksi? <i>Kysymyksellä arvioidaan: Onko organisaatiolla menetelmät valvoa turvallisuustilannetta ja menetelmät sekä valmius suojaavien ja korjaavien toimenpiteiden tekemiseksi.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatiossa on tunnettava tapa raportoida turvallisuuspoikkeamat. Turvallisuuspoikkeamien esiintymistä on valvottava.</p>	<p>TULOS & HAVAINNOT Toimintamalli on olemassa, perehdytetty ja ohjeistettu, mutta ei ole varmistuta tiedonkulusta, kun toimintaa ei seurata ja valvota koko ajan. Poikkeamatiedoille ei ole omaa järjestelmää, vain yhteinen toimintamalli. Turvallisuudesta vastaavalle lähetetään kaikki tieto ja joka vastaa toimenpiteistä ja viestinnästä. Poikkeamatietojen reagointimenettelytapaa ei ole määritetty eikä suunniteltu sekä miten seuranta ja tilannekuvaa ylläpidetään. Työturvallisuuden puitteissa seuranta päällä ja toimintamalli on olemassa, mutta suunnitelmalista reagointimenettelyä ei ole.</p>

Onnettomuudet, vaaratilanteet, turvallisuuspoikkeamat ja ennalta ehkäisevät toimenpiteet, A600

A600 (2 / 2)

<p>A 605.0</p> <p>Onko organisaatiolla menetelmät sen varmistamiseksi, että tehdyt suojaavat ja korjaavat turvallisuustoimenpiteet ovat tehokkaita ja oikein kohdistettuja?</p> <p><i>Kysymyksellä arvioidaan: Tehdäänkö turvallisuuden saavuttamiseksi oikeita asioita.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuustoimenpiteiden vaikutus arvioidaan ja organisaatiolla on käsitys panos-tuotos -suhteesta.</p>	<p>TULOS & HAVAINNOT</p> <p>Ei ole turvallisuus- tai suojaustoimenpiteiden tehokkuusarviointiin käytettäviä menettelyjä tai vaikutusten analysointimenetelmiä käytössä.</p>
<p>A 606.0</p> <p>Onko organisaatiolla menetelmät arvioida riskit, joita suunnitellut korjaavat toimenpiteet aiheuttavat?</p> <p><i>Kysymyksellä arvioidaan: Varmistaako organisaatio turvallisuusjärjestelmiä muutettaessa, ettei samalla aiheuteta uusia uhkia tai vaaratilanteita.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuustoiminnan prosessi sisältää arvion muutosten negatiivisista vaikutuksista.</p>	<p>TULOS & HAVAINNOT</p> <p>Ei huomioida muutosprosessien negatiivisia vaikutuksista. Ei varmisteta, että muutoksessa voidaan aiheuttaa uusia uhkia tai vaaratilanteita.</p>
<p>A 607.0</p> <p>Onko organisaatiolla menetelmät turvallisuustoimenpiteiden vaikutusten analysointia varten?</p> <p><i>Kysymyksellä arvioidaan: Dokumentoiko ja analysoiko organisaatio turvallisuustoimenpiteet sekä niiden vaikutukset.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatio seuraa turvallisuustoimenpiteiden vaikutuksia.</p>	<p>TULOS & HAVAINNOT</p> <p>Ei ole turvallisuus- tai suojaustoimenpiteiden tehokkuusarviointiin käytettäviä menettelyjä tai vaikutusten analysointimenetelmiä käytössä.</p> <p>Vaikutavuuarviointeja ja analysointiteja ei havaittu tehtävän.</p>
<p>A 608.0</p> <p>Onko organisaatiossa menettely, jonka avulla varmistetaan, että merkittävät tietojenkäsittelyympäristön muutokset tapahtuvat hallitusti?</p> <p>(ex I 109.0) Huom! Vaadittava toteutustapa riippuu kohteesta. Katso lisätietoja liitteestä 1 (A 608.0)</p>	<p>Elinkeinoelämän suositukset:</p> <p>Tietojenkäsittelyyn liittyviin muutoksiin on käytössä muutoshallintamenettely</p>	<p>TULOS & HAVAINNOT</p> <p>Tietoteknisten muutosten hallinnassa ei käytetä tietojenkäsittelyyn soveltuvia muutoshallintamenetelmiä.</p>
<p>Lähde/lisätieto</p> <p>ISO/IEC 27002 Luku 12 ja 10.1.2, PCI DSS 6.4, COBIT 4.1 A16, VAHTI 2/2010, VAHTI 3/2010, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschrift/guidelines/guidelines_pdf.pdf</p>		

Turvallisuuskirjoitukset ja sen hallinta, osa-alue A700

<p>A 701.0 Onko organisaatiolla toimintamallit, jotka koskevat:</p> <p>a. turvallisuustiedostoja / turvallisuus-rekistereitä tai dokumentointimenetelmiä? b. turvallisuuskirjoituksen tietojen yksilöintiä ja jäljittämistä? c. turvallisuuskirjoituksen säilyttämisaikoja, säilytyspaikkaa ja säilytyksen vastuuta?</p> <p><i>Kysymyksellä arvioidaan: Onko organisaatiolla järjestelmä, jonka avulla hallitaan edellä mainitut osatekijät.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatiolla on järjestelmä, joka sisältää omat ohjeistot ja tapahtumat turvallisuuspoikkeamat.</p>	<p>TULOS & HAVAINNOT Toimintamalli on olemassa, perehdytetty ja ohjeistettu, mutta ei ole varmistuta tiedonkulusta, kun toimintaa ei seurata ja valvota koko ajan. Poikkeamatiedoille ei ole omaa järjestelmää, vain yhteinen toimintamalli. Turvallisuudesta vastaavalle lähetetään kaikki tieto ja joka vastaa toimenpiteistä ja viestinnästä.</p> <p>Malli on jokaisen vastuuhenkilön oma arkistointitapa, jota ei ole ohjeistettu tai dokumentoitu.</p> <p>Omien tehtäväalueiden mukaisia käytäntöjä, joita ei yhteisellä ohjeistuksella ole selkeytetty. Turvallisuuskirjoitusten vastuumäärittelyt puuttuvat (omistaja + käyttö-ympäristö + säilytys + aika jne.).</p>
<p>A 702.0 Sisältävätkö rekisterit myös tiedot turvallisuustavoitteiden saavuttamisen tasosta?</p> <p><i>Kysymyksellä arvioidaan: Onko mitattavat tavoitteet asetettu selkeästi ja onko tavoitteiden toteutuminen helposti todettavissa järjestelmän avulla.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatio pystyy osoittamaan turvallisuustavoitteiden saavuttamisen tason vähintään vuosittain.</p>	<p>TULOS & HAVAINNOT Ei seurata toteumatilaa vuosittain. On vain työturvallisuusprojekteja ja hankkeita.</p> <p>Johdon tulostietoa ei käytetty, tavoitteita ei aseteta realistisesti mitattaviksi, joita ei myöskään mittareilla seurata. Tavoitteita asetetaan työturvallisuusasioissa.</p> <p>Ei ole yhtenäistä järjestelmää, vastuualueilla omat tavat seurata ja todeta toimintatason.</p>
<p>A 703.0 Sisältävätkö turvallisuusrekisterit tiedot annetuista turvallisuuskoulutuksista? <i>Kysymyksellä arvioidaan: Rekisteröidäanko turvallisuuskoulutukset siten, että niiden riittävyys ja voimassaolo voidaan todeta. Onko asetetut vaatimukset täytetty.</i></p>	<p>Elinkeinoelämän suositukset: Organisaatiolla on koulutusrekisteri, jolla voidaan osoittaa annettu koulutus ja sen sisältö.</p>	<p>TULOS & HAVAINNOT</p>
<p>A 704.0 Voitane dokumentaation perusteella osoittaa, että turvallisuuskoulutuksen taso on riittävän korkea? <i>Kysymyksellä arvioidaan: Onko turvallisuuskoulutukselle asetettu määrälliset ja laadulliset tavoitteet ja rekisteröidäanko niiden täyttyminen.</i></p>	<p>Elinkeinoelämän suositukset: Organisaation koulutusrekisteriin on kirjattu tasovaatimukset ja niiden toteutuminen varmistetaan siten, että työtehtävää ei aloiteta ennen koulutusvaatimuksen täyttymistä.</p>	<p>TULOS & HAVAINNOT</p>

Turvallisuskoulutus, tietoisuuden lisääminen ja osaaminen, osa-alue A800

A800 (1/2)

<p>A 801.0</p> <p>Ovatko organisaation kaikki henkilöt tietoisia turvallisuusvaatimusten noudattamisen tärkeydestä ja oikeista toimintatavoista?</p> <p><i>Kysymyksellä arvioidaan: Organisaation turvallisuuskulttuurin kypsyyttä ja johdon sitoutumista turvallisuuden jatkuvaan parantamiseen kouluttamisen avulla.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaation koko henkilöstö on koulutettu henkilöstö-, tila- ja tietoturvallisuuden vaatimuksien osalta. Erillisin projekteihin osallistuva henkilöstö on koulutettu projektikohtaisten vaatimusten mukaisesti.</p>	<p>TULOS & HAVAINNOT</p> <p>Kaikissa asioissa ei vielä ole saavutettu yhteneväistä tietoisuutta kiellimuurien ja toimintatapaerojen takia. Eritasoisten perehdytyksen osa-ongelma.</p> <p>Tietoturvasuosituksesta täydennettävä, lisättävä ja koulutuksen tasoa parannettava ja varmistettava että on todella koulutettu ja perehdytetty (+ sitoutuminen jatkuvaan turvallisuuden parantamiseen).</p>
<p>A 802.0</p> <p>Onko varmistuttu siitä, että henkilöstö tuntee omaan työhönsä liittyvät turvallisuusriskit?</p> <p><i>Kysymyksellä arvioidaan: Onko turvallisuusasioiden riskienarviointi toteutettu siten, että henkilöstö on itse mukana arvioinnissa ja tuntee työhönsä liittyvät turvallisuusriskit.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Riskienarvioinnin yhteydessä käsitellään ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueita koskevat seikat. Henkilöstölle selvitetään sen tehtäviin liittyvät turvallisuusriskit.</p>	<p>TULOS & HAVAINNOT</p> <p>Tietoturvallisuuden riskejä ei ole tunnistettu riittävällä tasolla. Riskienarviointi ei huomioi tietoturvallisuuden osa-alueita eikä ulkoistettua IT-palveluntuottajaa.</p>
<p>A 803.0</p> <p>Onko varmistuttu siitä, että henkilöstö osaa toimia oikein tilanteissa, joissa turvallisuus on vaarantunut?</p> <p><i>Kysymyksellä arvioidaan: Poikkeustilanteiden turvallisuusriskien hallintaa, esimerkiksi tilaturvallisuuden osalta tilipalotilanteet, tietoturvallisuuden osalta tietojen palauttamisen periaatteet.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiolla on tiedossaan sitä uhkaavat keskeiset turvallisuusriskit. Tärkeimpiin poikkeamatilanteisiin on dokumentoidut toimintamallit ja niistä keskeisimpiä harjoitellaan.</p>	<p>TULOS & HAVAINNOT</p> <p>Yrityksen turvallisuusriskejä ei ole kartoitettu ja tunnistettu liiketoiminnan jatkuvuuden sekä kokonaisturvallisuuden näkökulmasta.</p> <p>Turvallisuuspoikkeamatilanteita ei ole toimintamalleina dokumentoitu ja tärkeimpiä menettelytapoja ei harjoitella. Toimitaan pääsääntöisesti asiakkaan tiloissa ja poikkeamatilanteisiin annettujen koulutuksien ehdoilla.</p>
<p>A 803.1</p> <p>Miten organisaatiossa valvotaan tietoturvaohjeiden noudattamista?</p> <p><i>Lisäkysymys: Onko tietoturvarikkomusten käsittely ja seuraukset määritellyt?</i></p> <p>(ex I 206.0)</p> <p>Lähde/lisätieto a ISO/IEC 27002 8.2.3, VAHTI 8/2006</p>	<p>Elinkeinoelämän suositukset:</p> <p>Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan.</p> <p>Voidaan todentaa selvittämällä</p> <p>a. miten valvonta käytännössä toteutetaan,</p> <p>b. millaisia rikkeitä on tullut viime vuosina esille, ja</p> <p>c. miten rikkeisiin on puututtu.</p>	<p>TULOS & HAVAINNOT</p> <p>Tietoturvaohjeiden noudattamista valvotaan ja rikkeisiin puututaan hyvin vaihtelevasti.</p> <p>Tietoturvarikkomusten käsittelyä, sanktiointia ja menettelytapoja ei ole määritellyt. Seuraamuksien toteuttamisessa käytetään työsuhdetoimenpiteitä ja -menettelyjä.</p>

Turvallisuuskoulutus, tietoisuuden lisääminen ja osaaminen, osa-alue A800

A800 (2/2)

A 804.0	Elinkeinoelämän suositukset:	TULOS & HAVAINNOT
<p>Onko organisaatiolla menetelmä varmistaa siitä, minkä tasoista turvallisuuskoulutusta henkilöstö tarvitsee tehtävissään?</p> <p><i>Kysymyksellä arvioidaan: Onko organisaatiolla prosessi, jossa arvioidaan annettavan koulutuksen tarve huomioiden lakien vaatimukset, riskien arviointien perusteella annettavat keskeiset turvallisuusasiat ja yleiset turvallisuustietoisuuden vaatimukset.</i></p>	<p>Organisaatiolla on toiminto, joka määrittää turvallisuuskoulutuksen tasovaatimukset ainakin henkilöstö-, tila- ja tietoturvallisuuden osa-alueiden osalta.</p>	
<p>A 805.0</p> <p>Onko organisaatiolla menetelmä varmistaa, että työntekijöillä on tehtävien edellyttämä sopivuus, turvallisuuskoulutus, tehtävään perehtyminen ja kokemus?</p> <p><i>Kysymyksellä arvioidaan: Turvallisuus-koulutustason selvittämisen mahdollisuutta.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuuskoulutusrekisteristä saadaan tieto tehtävän edellyttämästä turvallisuuskoulutustasosta.</p>	
<p>A 806.0</p> <p>Miten organisaatiossa on huolehdittu riittävästä ohjeistuksesta, koulutuksesta ja tiedotuksesta?</p> <p>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschtz/guidelines/guidelines_pdf.pdf</p> <p>Lähde lisätietoa</p> <p>ISO/IEC 27002 10.7.3, ISO/IEC 27002 13.1.1, ISO/IEC 27002 7.2.2, ISO/IEC 27002 8.2.2, PCI DSS 12.6, COBIT 4.1 DS7, Kansallisen turvallisuusviranomaisen "Kansainvälisen turvallisuusluokitellun tietosäestön käsittelyohje", VAHTI 8/2006, EU:n turvallisuussäännöstö 6952/2/11 REV2 /1.4.2011 liite I, VAHTI 2/2010, VAHTI 3/2010,</p> <p>https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschtz/guidelines/guidelines_pdf.pdf</p> <p>Voidaan todentaa esim. siten, että kysellään muutamalta tarkastuksen yhteydessä satunnaisesti valitulta käyttäjältä, miten heidät on ohjeistettu toimimaan tietoturvallisesti.</p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaatiossa on huolehdittu riittävästä ohjeistuksesta ja koulutuksesta. Henkilöstö on saanut perehdytyksen yhteydessä ohjeet, kuinka toimia organisaation turvaperiaatteiden mukaisesti.</p> <p>Ohjeistuksen/koulutuksen tulee sisältää tärkeimmät toimintatilanteet (peruskäyttö, etäkäyttö, matkatyö, ylläpito, jne.) ja -tavat.</p>	<p>TULOS & HAVAINNOT</p> <p>Tietojen ja ohjeiden perillemenossa vaikeuksia ja vaihtelevuutta (kieli + kulttuurierot).</p> <p>Perehdytystaso vaihtelee perehdyttäjän mukaan ja kaikkia asioita ei käydä läpi täydessä laajuudessa.</p> <p>Yleisohjeistus kattaa verkon, sähköpostin ja internetin hyvän käytötavan mukaiset säännöt, mutta ei tietoturvanäkökulmasta.</p>
<p>A 807.0</p> <p>Onko tietoon ja tietojenkäsittelypalveluihin määritetty hyväksyttävän käytön säännöt ja onko niistä tiedotettu henkilöstölle? (ex I 205.0)</p> <p>Lähde lisätietoa</p> <p>ISO/IEC 27002 7.1.3, PCI DSS 12.3, VAHTI8/2006</p> <p>Voidaan todentaa tarkistamalla AUP:n (acceptable use policy) olemassaolo ja sisältö, lisäksi se, onko AUP helposti saatavilla henkilöstölle. Selvitetään lisäksi miten AUP:sta tiedotettu henkilöstölle.</p>	<p>Elinkeinoelämän suositukset:</p> <ol style="list-style-type: none"> 1) Tiedon ja tietojenkäsittelypalveluihin liittyvien suojattavien kohteiden hyväksyttävän käytön säännöt on määritetty. 2) Hyväksyttävän käytön säännöissä otetaan kantaa vähintään siihen, saako organisaation tietojärjestelmiä käyttää henkilökohdaisiin tarpeisiin (sähköposti, levytila, pankkipalveluiden käyttö, jne.). 3) On selkeästi tiedotettu hyväksyttävän käytön säännöistä henkilöstölle. 4) Hyväksyttävän käytön säännöt ovat henkilöstölle helposti saatavilla. 	

Raportointi ja johdon katselmuksat, osa-alue A900

<p>A 901.0</p> <p>Raportoiko turvallisuudesta vastaava henkilö suoraan organisaation ylimmälle johdolle turvallisuuteen liittyvissä asioissa?</p> <p><i>Kysymyksellä arvioidaan: Johdon sitoutumista turvallisuustyöhön.</i></p> <p><i>Onko turvallisuusjohdolla suora nopea ja tehokas yhteyskanava organisaation johtoon?</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuudesta vastaava henkilö raportoi organisaation johdolle säännöllisesti siten, että johtoryhmä on selvillä turvallisuustoiminnan ja turvallisuustilanteen tasosta. Huomattavat poikkeamat tai muutokset on voitava raportoida johdolle välittömästi esimerkiksi kriisinhallintamenettelyn kautta.</p>	<p>TULOS & HAVAINNOT</p> <p>Turvallisuuden tilannekuvan ylläpitoa, tiedon kulkua ei ole testattu, realistisesti arvioitu ja varmistettu.</p> <p>Huomattavien poikkeamatilanteiden varalle ei ole luotu kriisinhallintamenettelyä. Löytyy poikkeamatilanteita varten tehty ohjeistus, ilmoituslomake ja lähetysohje.</p>
<p>A 902.0</p> <p>Tarkastaako organisaation ylin johto säännöllisesti (vähintään kerran vuodessa) turvallisuusjärjestelmän toimivuuden?</p> <p><i>Kysymyksellä arvioidaan: Organisaation johdon sitoutumista turvallisuustyön jatkuvaan parantamiseen ja laadukkaaseen johtamiseen.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Vähintään vuosittainen turvallisuusasioiden raportointi on järjestetty osaksi muuta johtamisprosessia.</p>	<p>TULOS & HAVAINNOT</p>
<p>A 903.0</p> <p>Arvioidaanko ylimmän johdon tekemissä tarkastuksissa turvallisuusjärjestelmän soveltuvuus, resurssien riittävyys ja toiminnan tehokkuus?</p> <p><i>Kysymyksellä arvioidaan: Raportoinnin laatu ja laaja-alaisuus.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Organisaation turvallisuustavoitteet ja tavoitteiden saavuttaminen esitetään mitattavassa muodossa.</p>	<p>TULOS & HAVAINNOT</p> <p>Johdon tulostarkastuksia ei käytetty, tavoitteita ei aseteta realistisesti mitattaviksi, joita ei myöskään mittareilla seurata. Tavoitteita asetetaan työturvallisuusasioissa.</p> <p>Kyseinen auditointi oli ensimmäinen eli ei säännöllistä ja suunnitelmallista sisäistä toimintaa.</p>
<p>A 904.0</p> <p>Dokumentoidaanko tehdyt seurantatarkastukset?</p> <p><i>Kysymyksellä arvioidaan: Organisaation johdon systemaattista toimintaa ja mahdollisuutta tarkastella seurannan perusteella tehtyjen ratkaisujen vaikutusta ja tehokkuutta.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Seurantatarkastukset dokumentoidaan.</p>	<p>TULOS & HAVAINNOT</p> <p>Kyseinen auditointi oli ensimmäinen turvallisuusjohtamisjärjestelmästä tehty arviointitarkastus.</p>
<p>A 905.0</p> <p>Toimivatko nämä seurantatarkastukset jatkuvan parannuksen perustekijöinä, eli vaikuttavatko ne politiikan ja tavoitteiden sisältöön?</p> <p><i>Kysymyksellä arvioidaan: Muodostaako turvallisuusjohtaminen laadukkaan toiminnan, jossa politiikka ja tavoitteet sekä turvallisuuden toimintamallit ovat jatkuvan parantamisen kohteina.</i></p>	<p>Elinkeinoelämän suositukset:</p> <p>Turvallisuusjohtamiseen kuuluu prosessi, jossa johdon palautetta käytetään turvallisuuspolitiikan ja tavoitteiden uudelleenarvioimisessa.</p>	<p>TULOS & HAVAINNOT</p> <p>Koska ei ole aikaisemmin tehty, ei ole myöskään käytetty saatuja tuloksia turvallisuusasioiden uudelleenarvioinnissa.</p>

KATAKRI III - Hallinnollinen turvallisuus (T osa-alue)
Turvallisuusjohtaminen

(Katakri III T 1/4)

T 01	Minimisuositukset:	TULOS & HAVAINNOT
Turvallisuusperiaatteet	1) Organisaatiolla on ylimmän johdon hyväksymät turvallisuusperiaatteet, jotka kuvaavat organisaation turvallisuustoiminnan kytkeytymistä organisaation toimintaan. 2) Turvallisuusperiaatteet ovat organisaation ja suojattavien kohteiden kannalta kattavat ja tarkoituksenmukaiset. 3) Turvallisuusperiaatteet ohjaavat turvallisuustoimintaa. Turvallisuusperiaatteiden toteutumisesta raportoidaan ja niiden toteutumista seurataan säännöllisesti.	TULOS & HAVAINNOT Yrityksen ylimmän johdon (näkyvät) allekirjoitukset ja hyväksyntä puuttuvat turvallisuuspolitiikasta. Mainitaan johdon tulokortti, jota kuitenkaan ei ole olemassa. On huomioitu ainoastaan kohteiden riskit. Yritykselle ja liiketoiminnalle tärkeät suojattavat kohteet on määrittelemättä. Ainoastaan työ-, henkilöstö- ja paloturvallisuudessa asetetaan tavoitteita. Johdon tuki ja hyväksyntä puuttuvat ja turvallisuustoiminta tapahtuu työturvallisuuden näkökulmasta.
Organisaation turvallisuusperiaatteilla tavoitellaan sitä, että johto sitoutuu organisaation turvallisuustyöhön ja että turvallisuustyö tukee organisaation toimintaa. Turvallisuusperiaatteet viestitään henkilöstölle ja tarvittaville sidosryhmille. Periaatteet voidaan kuvata monin eri tavoin, esimerkiksi ISO/IEC 27002:2013 5.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; ISO/IEC		

T 02	Minimisuositukset:	TULOS & HAVAINNOT
Turvallisuustyön tehtävien ja vastuiden määrittäminen	1) Organisaatio on määritellyt turvallisuuden hoitamisen tehtävät ja vastuut ainakin seuraavilta osin: a) turvallisuuden hallinta b) henkilöstöturvallisuus c) fyysinen turvallisuus d) tietotekninen turvallisuus 2) Vastuumäärittely sisältää salassa pidettävän tiedon käyttöympäristön omistajan sekä turvallisuuteen liittyvät vastuut. 3) Turvallisuusdokumentaation kattavuuden ja ajantasaisuuden säännöllinen seuranta on vastuutettu. Turvallisuusdokumentaatio kattaa salassa pidettävään tietoon liittyvät prosessit ja käsittelyympäristöt koko tiedon elinkaaren ajalta, ja se on tarvittavien tahojen saatavilla.	TULOS & HAVAINNOT Turvallisuusjohtamisessa ja -organisaatiossa ei riittävästi huomioida kokonaisvaltaisuutta, järjestelmällisyyttä ja säännöllistä vuosikello kiertoa. Ei huomioida riittävästi tietoturvaluutta, joka on merkittävä asia, koska se vaikuttaa myös toiminnan haavoittuvuuteen sekä jatkuvuudenhallintaan. Asiakirjavastuumäärittelyt puuttuvat kokonaan (omistaja+käyttöympäristö). Omien tehtäväalueiden mukaisia käytäntöjä, joita ei yhteisellä ohjeistuksella ole selkeytetty. Turvallisuusdokumentaatioiden vastuumäärittelyt puuttuvat (omistaja + käyttöympäristö + säilytys + aika jne.).
Turvallisuustyön tehtävien ja vastuiden määrittelyllä pyritään varmistamaan, että keskeisimpiin osa-alueisiin on nimetty tekijät ja heillä on tiedossaan omat vastuunsa ja valtuutensa. ISO/IEC 27002:2013 6.1.1; ISO/IEC 27001:2013 5.1; ISO/IEC 27001:2013 5.2; ISO/IEC 27001:2013 5.3; VAHTI 2/2010		

T 03	Minimisuositukset:	TULOS & HAVAINNOT
Turvallisuustyön resurssit	Organisaatiolla on käytössään riittävä asiantuntemus tietoturvallisuuden varmistamiseksi. Riittävällä asiantuntemuksella pyritään varmistamaan, että tietoturvallisuustyön tarkoitus toteutuu ja toimet mitoitetaan kustannustehokkaasti. Resurssien riittävyttä arvioidaan säännöllisesti.	TULOS & HAVAINNOT Tietohallinnossa riittämätön resursointi ja asiantuntemus, tietoturvaluudesta vastaavaa ei ole nimetty, vastuutettu eikä valtuuksia annettu.
ISO/IEC 27001:2013 7.1; ISO/IEC 27001:2013 7.2; ISO/IEC 27001:2013 5.1; VAHTI 2/2010		

KATAKRI III - Hallinnollinen turvallisuus (T osa-alue)

(Katakri III T 2/4)

Turvallisuusjohtaminen

T 04	Minimisuositukset:	TULOS & HAVAINNOT
Turvallisuusriskien hallinta	1) Organisaatiolla on käytössä riskienhallintaprosessi. Riskienhallinnan on oltava säännöllinen ja jatkuva, dokumentoitu prosessi. Riskienhallinnan periaatteet on kuvattu.	Ei ole käytössä riskienhallintaprosessia, vakiintunutta ja järjestelmällistä menetelmää.
Riskienhallinta on organisaation johdon ja muun henkilöstön toteuttama organisaation johtamiseen ja toimintaan sisältyvä prosessi, jota sovelletaan riittäväksi katsottavissa määrin kaikessa organisaation toiminnassa (esimerkiksi prosessit, asiakassuhteet). Riskienhallinnan tavoitteena on tunnistaa ja hallita organisaation toimintaedellytyksiä mahdollisesti vaarantavia tekijöitä ja pitää toimintaan kohdistuvat riskit sellaisissa rajoissa, etteivät organisaation toiminta ja tavoitteet ole uhattuna.	2) Riskien analysoinnissa on käytettävä vakiintunutta, avointa ja ymmärrettävää järjestelmällistä menetelmää. Suojattavat kohteet on tunnistettu.	Ei havaittu riskienarviointien tekemistä tai vuosittaista päivitysten säännönmukaisuutta. Tehdyt arvioinnit kohteista dokumentoitu.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	3) Riskienhallintaan osallistuvat tarvittavat tahot organisaation sisältä ja ulkopuolelta. Suojattaville kohteille on nimetty omistaja/vastuhenkilö.	Tietoturvallisuuden riskejä ei ole tunnistettu riittävällä tasolla. Riskienarviointi ei huomioi tietoturvallisuuden osa-alueita eikä ulkoistettua IT-palveluntuottajaa.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	4) Riskienhallinnan on katettava vähintään turvallisuusjohtamisen, tila- ja tietoturvallisuuden osa-alueet. Tunnistetut riskit on otettava huomioon tarvittavien sidosryhmien osalta. Organisaation tulee varmistaa, että salassa pidettäviä tietoja koskevia velvoitteita noudatetaan myös tilanteissa, joissa tietoja käsitellään organisaation toimeksiantoissa. Suojattaviin kohteisiin liittyvät riskit on tunnistettu ja arvioitu.	Riskien arviointi tapahtuu kohteessa ja siihen liittyviin sidosryhmiin. Riskienarviointi ei huomioi tietoturvallisuuden osa-alueita eikä ulkoistettua IT-palveluntuottajaa.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	5) Riskienhallintaprosessia ja sen tuloksia hyödynnetään organisaation turvallisuustavoitteiden asettamisessa, turvallisuuspoikkeamien vaikutusten arvioinnissa, turvatoimien suunnittelussa, muutoksenhallinnassa ja soveltuvilta osin hankintamenettelyissä. Suojausmenetelmät on suhteutettu tunnistettuihin riskeihin.	Ei olla varmistettu eikä dokumentoitu, että salassa pidettäviä tietoja koskevia velvoitteita noudatettaisiin.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	6) Turvatoimet on mitoitettu ottaen huomioon muun muassa tiedon suojaustaso, määrä, muoto, luokitteluperuste ja sijoitustilat suhteessa arvioitun vihameiäisen tai rikollisen toiminnan uhkaan. Riskienhallintaan ja analysointiin käytetään jotain järjestelmällistä menetelmää.	Riskienarvioita tehdään kohteissa työturvallisuuden näkökulmasta, joka on myös lähtökohtana turvallisuustyölle. Riskienhallintaprosessin puuttuessa ei voida todeta näin tapahtuneen.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	7) Organisaatio dokumentoi keskeisiltä osin sovellettavat valvonta- ja turvatoimet. Organisaatiossa ylläpidetään kuvausta turvallisuusjärjestelyistä. Riskienhallintaprosessin johtopäätökset on huomioitu organisaation turvallisuusdokumentaatioissa.	Työturvallisuusasioissa työsuojelutoimikunta huomioi riskiarvioinneissa tehtyjä havaintoja tavoitteita asettaessa. Kattaa vain henkilö-, tila- ja työturvallisuusasiat.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnan kohdentaminen viranomaisen salassa pidettävien tietojen näkökulmasta	Riskienhallintaprosessin käytön ja olemassaolon puuttuessa ei voida todeta näin tapahtuneen.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Tiedon suojaustasoa ei ole huomioitu ja luokiteltu eikä suojaustasoa määritetty.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Tehokkuusanviointia ei ole toteutettu eikä analysoitu toteutettujen toimenpiteiden vaikuttavuutta. Suojauksien toteutuksen tehokkuutta ja vaikutuksia ei seurata, arvioida eikä tuloksia dokumentoida, kuin työturvallisuuden osa-alueessa.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Ei dokumentaatiota esitetty.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Uhkien tunnistus kohdistuu henkilö- ja työturvallisuuden suojauksiin sekä as.kohteisiin ja kohteesta vastaa kohde esimies. Yrityksen toiminnalle tärkeitä suojattavia kohteita eikä riskejä ole tunnistettu tai määritetty.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.
Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.	Riskienhallinnalla tarkoitetaan kaikkea organisaatiossa tehtävää toimintaa riskien ja niistä aiheutuvien vahinkojen vähentämiseksi. Riskienhallinta on tilanteiden arviointia, suunnittelua ja käytännön tekoja, johon osallistuu kukin henkilöstön jäsen omassa roolissaan. Hyvä riskienhallinta on luonteeltaan ennakoivaa, tietoista, suunnitelmallista ja järjestelmällistä.

KATAKRI III - Hallinnollinen turvallisuus (T osa-alue)

(Katakri III T 3/4)

Turvallisuusjohtaminen

<p>T 04 jatkuu...</p> <p>Riskienhallintatoimet tulee kohdentaa siihen ympäristöön, jossa salassa pidettäviä tietoja on tarkoitus käsitellä. Tietojenkäsittely-ympäristöön sisältyy yleensä sekä henkilöstöön, toimitiloihin että tietojärjestelmiin liittyviä kokonaisuuksia.</p> <p>ISO/IEC 27001:2013 6.1.2; ISO/IEC 27001:2013 6.1.3; ISO/IEC 27001:2013 6.2; ISO/IEC 27001:2013 8.2; ISO/IEC 27001:2013 8.3; ISO/IEC 27001:2013 9.1; ISO/IEC 27001:2013 9.3; ISO/IEC 27001:2013 10.1; ISO/IEC 27002:2013 8.1.1; ISO/IEC 27002:2013 8.1.2; ISO/IEC 27002:2013 18.1.1; ISO/IEC 27002:2013 18.2.2; ISO/IEC 27002:2013 18.2.1; ISO/IEC 27005:2011; ISO 31000:2009; OCTAVE Allegro; SRHY-riskienhallinta; VTT - Riskianalyysimenetelmät; VAHTI 2/2010.</p> <p><u>Monitasoisen suojaamisen huomiointi riskienhallinnassa</u></p> <p>Riskienhallinnassa tulee huomioida turvallisuusjärjestelyjen monitasoisuus. Yksittäisiin riskeihin nähden riittävän suojauksen voi toteuttaa yksittäisillä luotettavilla turvatoimilla, tai useampia</p> <p><u>Riskien hallinnan ja analysoinnin menetelmiä</u></p> <p>Useita eri menetelmiä, jotka perustuvat uhkien ja haavoittuvuuksien tunnistamiseen, todennäköisyyksien ja vaikuttavuuden arviointiin, tarvittavien riskien pienentämistoimenpiteisiin,</p>	<p><u>Minimisuositukset:</u></p>	<p>TULOS & HAVAINNOT</p> <p>Yrityksen toiminnalle tärkeillä suojattavilla kohteilla ei ole omistajaa.</p> <p>Työsuojelutoimikunta käsittelee suojaustoimintojen asianmukaisuutta työturvallisuusasioissa. Ei ole dokumentoitu suojaustoimien päätös tai hyväksymis asiakirjoja.</p> <p>Kohdekansioon liitetään kohteesta tehty riskienarviointilomake.</p>
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>T 05</p> <p>Turvallisuusriskien hallinta</p> <p>Organisaatiossa on tunnistettu riippuvuudet ulkoisista tekijöistä, ja niiden vaikutuksista omaan toimintaan. Organisaatiossa on tunnistettu oman toiminnan vaikutus muihin.</p>	<p><u>Minimisuositukset:</u></p> <ol style="list-style-type: none"> 1) Toipuminen ja jatkuvuuden varmistaminen toimintavaatimukseen nähden riittävässä ajassa on huomioitu suunnittelussa. 2) Toiminnan jatkuvuus suunnitelmiin on sisällytettävä ennalta ehkäiseviä ja korjaavia toimenpiteitä, jotta minimoitaisiin merkittävien toimintahäiriöiden tai poikkeuksellisten tapahtumien vaikutukset salassa pidettävien tietojen käsittelyyn ja säilyttämiseen. 3) Poikkeamista tehdyt havainnot tuodaan osaksi riskienarviointia ja tarpeen mukaan näiden pohjalta päivitetään toipumis- ja jatkuvuus suunnitelmia. 4) Jatkuvuuden varmistamiseen liittyvissä suunnitelmissa on otettu huomioon tarve suojata tiedot hätätilanteissa, jotta estetään luvaton pääsy tietoihin, tietojen ilmitulo tai niiden eheyden tai käytettävyyden menettäminen. 	<p>TULOS & HAVAINNOT</p> <p>Ei ole toteutettu toipumis- ja jatkuvuus suunnitelmia.</p> <p>Ei ole toteutettu toipumis- ja jatkuvuus suunnitelmia.</p> <p>Systemaattista poikkeamatietojen hyväksikäyttöä on, mutta ei ole varmistettu niiden kokonaisvaltaista ja tehokasta käyttöä.</p> <p>Ei ole varmuutta kaikkien tietojen kirjaamisesta ja tallentamisesta, johon tulisi panostaa enemmän.</p> <p>Ei ole toteutettu toipumis- ja jatkuvuus suunnitelmia.</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

ISO/IEC 27002:2013 17.1.1; ISO/IEC 27002:2013 17.1.2; ISO/IEC 27002:2013 17.2.1; ISO/IEC 27002:2013 12.3.1; ISO/IEC 27002:2013 16.1.2; ISO/IEC 27002:2013 16.1.6; VAHTI 2/2009; VAHTI

KATAKRI III - Hallinnollinen turvallisuus (T osa-alue)
Turvallisuusjohtaminen

(Katakri III T 4/4)

<p>T 06</p> <p>Turvallisuuspoikkeamien hallinta</p> <p>Turvallisuuspoikkeamien hallinnalla pyritään varmistamaan, että organisaatio kykenee toimimaan tehokkaasti ei-toivotuissa tilanteissa, minimoiden vahingot ja palauttaen tilanteen normaalkiksi. Tehokas poikkeamienhallinta edellyttää myös riittävää resursointia.</p> <p>Useat tiedon omistajat (esimerkiksi EU) sekä myös voimassa olevat viranomaishyväksynnät tai -todistukset edellyttävät välitöntä ilmoitusta salassa pidettävän tiedon vaarantaneista poikkeamista tai</p> <p>ISO/IEC 27002:2013 16.1.1; ISO/IEC 27002:2013 16.1.2; ISO/IEC 27002:2013 16.1.4; ISO/IEC 27002:2013 16.1.5; ISO/IEC 27002:2013 6.1.3; VAHTI 2/2010</p>	<p>Minimisuositukset:</p> <p>1) Organisaatiolla on menettelytavat turvallisuuspoikkeamien asianmukaiseen käsittelyyn.</p> <p>2) Organisaatio on määrittänyt henkilöt/tahot, joille turvallisuuspoikkeamista tai niiden epäilyistä tulee ilmoittaa.</p> <p>Turvallisuuspoikkeamien hallinta on</p> <p>1) suunniteltu, 2) ohjeistettu/koulutettu, 3) dokumentoitu käyttöympäristöön nähden riittävällä tasolla, 4) harjoiteltu, ja erityisesti 5) viestintäkäytännöt ja vastuut on sovittu.</p>	<p>TULOS & HAVAINNOT</p> <p>Poikkeamatietojen reagointimenettelytapaa ei ole määritelty eikä suunniteltu sekä miten seuranta ja tilannekuvaa ylläpidetään. Työturvallisuuden puitteissa seuranta päällä ja toimintamallilla on olemassa, mutta suunnitelmalista reagointimenettelyä ei ole.</p> <p>Toimintamalli on olemassa, perehdytetty ja ohjeistettu, mutta ei ole varmistuta tiedonkulusta, kun toimintaa ei seurata ja valvota koko ajan. Poikkeamatiedoille ei ole omaa järjestelmää, vain yhteinen toimintamalli. Turvallisuudesta vastaavalle lähetetään kaikki tieto ja joka vastaa toimenpiteistä ja viestinnästä.</p> <p>Huomattavien poikkeamatilanteiden varalle ei ole luotu kriisinhallintamenettelyä. Löytyy poikkeamatilanteita varten tehty ohjeistus, ilmoituslomake ja lähetysosoite.</p> <p>Turvallisuuspoikkeamatilanteita ei ole toimintamalleina dokumentoitu ja tärkeimpiä menettelytapoja ei harjoitella. Toimitaan pääsääntöisesti asiakkaan tiloissa ja poikkeamatilanteisiin annettujen koulutuksien ehdoilla.</p> <p>Resurssien riittävyys ei ole testattu, sillä ei ole ollut sellaista tilannetta, jossa toimintaa olisi jouduttu palauttamaan normaalkiksi tms.</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>T 07</p> <p>Tietojen luokittelu</p> <p>ISO/IEC 27002:2013 8.2.1; ISO/IEC 27002:2013 8.2.2; VAHTI 2/2010</p> <p>Luokittelun tavoitteena on tunnistaa ja mitoitaa turvatoimet tiedon suojaustarpeen perusteella. Luokituksen voi ilmaista eri tavoin riippuen tietoaineistosta, käsittely-ympäristöstä ja käyttäjistä. Luokittelemalla tietojenkäsittely-ympäristöt tietoaineiston mukaisesti, pystytään selkeämmin osoittamaan ja perustelemaan kuhunkin tietojenkäsittely-ympäristöön liittyvät turvatoimet.</p>	<p>Minimisuositukset:</p> <p>Tiedot on luokiteltu lakisäateisten vaatimusten perusteella:</p> <p>a) Tietosisällöltään salassa pidettävät aineistot ja asiakirjat (ml. luonnokset) varustetaan suojaustasoa kuvaavalla merkinnällä.</p> <p>b) Asiakirja merkitään asiakirjan osien (esim. liitteet) ylintä suojaustasoa vastaavalla merkinnällä.</p> <p>c) Mikäli pääasiakirjan ja liitteiden luokitustaso ei ole sama, tämän on käytävä ilmi asiakirjasta.</p>	<p>TULOS & HAVAINNOT</p> <p>Turvaluokitettun aineistolle ja asiakirjoille ei ole laadittu ohjeistusta suojaus- tai luokitusmerkinnästä eikä käsittelyohjeita ole käytössä.</p> <p>Turvaluokitusta ei ole käytössä eikä asiakirjoja merkitä tai suojata.</p> <p>Ei ole tietojenkäsittely-ympäristön suojaustasoa mitoitettu.</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Turvallisuuskysely 2015

Kyselyvastausten mukaisessa puutteellisuus järjestyksessä

Sija	Kysymys ALUE	KATAKRin kysymyksen pääaihe (kriteeristö ja tavoite, joka tulee täyttää)	PA	Keeki-arvo	Keeki-hajonta	0 arvojen %-osuus	% OSUUUS
1	6060	Varmistusmenetelmä korjaustoimenpiteiden negatiivisista vaikutuksista	P	0,50	0,93	75,0 %	10,0 %
2	9040	Turvallisuustavoitteiden seuranta- ja tulokset dokumentoidaan	P	1,00	1,15	50,0 %	20,0 %
2	9050	Tarkastuspalauteiden mukaan turvallisuusjärjestelmiä arvioidaan uudelleen	P	1,00	1,15	50,0 %	20,0 %
4	4090	Tietoturvaluottelu huomioidaan alihankinta-, ostopalvelu- ja muussa yhteistyössä	P	1,13	1,39	58,3 %	22,5 %
5	6050	Arviointimenetelmä suojauksien tehokkuudesta ja kohdistuksen oikeellisuudesta	P	1,25	1,50	50,0 %	25,0 %
5	6080	Hallitussa tietojenkäsittely-ympäristössä on oma muutoksen hallintamenettely	P	1,25	1,50	50,0 %	25,0 %
7	T7	Tietoaineistot ovat luokiteltu ja merkattu lakisääteiden vaatimusten perusteella	P	1,30	0,98	35,0 %	26,0 %
8	4100	Tietoturvaopkeamissa toimitaan, viestitään ja dokumentoidaan suunnitellusti	P	1,45	1,82	51,4 %	29,0 %
9	3060	Tiedon käsittely-ymp. on suojattu luokituksen ja tietoturvaopkeamien mukaan	P	1,69	1,54	37,5 %	33,8 %
10	6030	Määritetty turvapoikkeamatilanteiden vaikutusten pienentämistä vastuut	K	1,75	1,18	25,0 %	35,0 %
11	T5	Jatkuvuus suunnitelmissa on ennaltaehkäiseviä ja minimoivia toimenpiteitä	P	1,79	1,71	43,8 %	35,8 %
12	3040	Turvallisuustoiminnan tavoitteille on asetettu realistiset aikataulut	P	1,94	1,72	40,8 %	38,8 %
13	8031	Tietoturvaopkeamien noudattamista valvotaan ja rikkeisiin puututaan	K	1,95	1,84	38,7 %	39,0 %
14	6070	Seuranta- ja korjaustoimenpiteiden vaikutusten analysoinnissa	P	2,00	1,31	25,0 %	40,0 %
15	4012	Riskejä arvioidaan vuosittain järjestelmällisesti ja johto on hyväksynyt suojaukset	K	2,03	1,83	33,2 %	40,7 %
16	8040	Varmistusmenetelmä henkilöstön turvallisuusopkeamien tasovaatimuksille	V	2,10	1,80	31,8 %	42,0 %
17	4070	Valvontamenetelmä toimenpiteiden tehokkuuden ja toteutuksen arviointiin	P	2,12	1,55	28,8 %	42,4 %
18	9030	Turvallisuustavoitteita mitattaroidaan (soveltuvuus, tehokkuus, riittävyys)	P	2,25	1,56	26,4 %	44,9 %
19	6010	Jatkuvuudenhallintamenettelyn mukaan on varauduttu, suojattu ja varmennettu	P	2,25	1,71	25,0 %	45,0 %
19	6020	Määritetty turvapoikkeamatilanteita johtava, käsiteltävä ja tutkiva henkilö	K	2,25	1,49	25,0 %	45,0 %
21	7020	Vuosittain osoitettu turvallisuustavoitteiden saavuttamistaso	K	2,25	1,57	27,2 %	45,0 %
22	3030	Turvallisuustoiminnalle on asetettu konkreettiset tavoitteet, joita voi mitata	P	2,27	1,82	28,8 %	45,3 %
23	8070	Hyväksyttävään käytön säännöt on määritetty, tiedotettu ja saatavilla helposti	K	2,27	1,83	27,6 %	45,4 %
24	4030	Riskienarviointitulokset päivitetään ja dokumentoidaan säännöllisesti vuosittain	K	2,28	1,48	22,4 %	45,5 %
24	8010	Turvallisuusvaatimusten täyttäminen ja noudattamisen tärkeys on koulutettu	K	2,28	1,28	14,3 %	45,5 %
26	T3	Tietoturvaluotteluun varmistamiseksi on riittävät resurssit ja asiantuntemus	P	2,31	1,60	26,5 %	46,1 %
27	2020	Kehitystavoitteista on toimintaohjelma, jossa menetelmät, vastuut ja aikataulut	K	2,33	1,57	26,5 %	46,5 %
27	4050	Riskienarviointitulosten perusteella priorisoidaan riskit tärkeysjärjestykseen	K	2,33	1,75	32,2 %	46,5 %
27	5030	Riittävästi resursseja turvallisuustyön toteutukseen, kontrolliin ja kehitykseen	K	2,33	1,20	10,2 %	46,5 %
30	4080	Tietoturvaluotteluun käytännön toteutuksen seuranta, arviointi ja kehittäminen	P	2,37	1,80	24,5 %	47,3 %
30	8050	Koulutusrekisteristä saadaan tieto tehtävän edellyttämästä koulutustasosta	V	2,37	1,80	26,5 %	47,3 %
32	5010	Turvallisuustyön vastuut on kattavasti määritetty ja nimetty koko organisaatiossa	K	2,39	1,58	25,6 %	47,8 %
33	9010	Turvallisuudesta vastaava raportoi säännöllisesti johtoryhmälle (tilannekuva)	K	2,41	1,81	25,5 %	48,2 %
34	2040	Tietoturvasuunnitelma (hallinnollinen, fyysinen ja tietotekninen) sekä tietosuojat	P	2,42	1,85	28,0 %	48,4 %
35	2030	Toimintaohjelman säännöllinen tarkastaminen on jatkuva johtamistyötä	K	2,43	1,83	26,5 %	48,6 %
36	3020	Turvallisuustavoitteet on asetettu kaikille hierarkiatasolle ja/tai toiminnolle	K	2,53	1,55	22,4 %	50,6 %
37	T8	Turvapoikkeamatilanteita varten on määritetty ja ohjeistettu ilmoitusmenettely	K	2,54	1,52	20,2 %	50,8 %
38	8060	Turvallinen toiminta perehdytetty, koulutettu ja tiedotettu eri toimintatilanteisiin	K	2,55	1,42	16,3 %	51,0 %
39	T4	Riskienhallintaprosessi säännöllinen, järjestelmällinen, laaja ja hyödynnettävissä	P	2,56	1,51	21,1 %	51,2 %
40	4020	Riskimenetelmät kattavat normaalin toiminnan, erityistilanteet ja hätätapaukset	K	2,58	1,56	21,4 %	51,6 %
41	8030	Henkilöstö osaa toimia oikein tilanteissa, joissa sen turvallisuus on vaarantunut	P	2,60	1,42	13,3 %	52,0 %
42	5011	Tietoturvasuunnitelma, tietoturvaopkeamat, koulutus, seuranta ja katselmointi	P	2,64	1,81	22,2 %	52,9 %
43	4011	Suojattavat kohteet ja uhat on tunnistettu, vastuutettu ja suojaukset laadittu	P	2,67	1,54	20,4 %	53,5 %
44	1040	Turvallisuuspolitiikan mukaista toimintaa seurataan ja valvotaan kaikkialla	P	2,69	1,37	14,3 %	53,7 %
45	4010	Säännöllinen ja dokumentoitu menetelmä tunnistaa ja arvioida turvallisuusriskejä	K	2,72	1,52	18,4 %	54,5 %
46	7010	Turvallisuusopkeamista löytyy kootut ohjeet ja tapahtumarekisteri	K	2,74	1,51	17,5 %	54,7 %
47	8020	Henkilöstö tuntee tai sille selvitetään sen tehtäviin liittyvät turvallisuusriskejä	K	2,77	1,39	13,3 %	55,3 %
48	2010	Kirjoitettu dokumentti turvallisuuden johtamiseksi ja tavoitteiden saavuttamiseksi	K	2,80	1,88	22,4 %	55,9 %
48	3010	Turvallisuuspolitiikka on perusteena turvallisuustyön tavoitteiden asettamiselle	P	2,80	1,57	18,4 %	55,9 %
50	4040	Riskienarviointitulosten mukaan asetetaan turvallisuustoiminnalle tavoitteita	K	2,84	1,43	16,3 %	56,7 %
51	9020	Vuosittainen turvallisuusasioiden raportointi on osa johtamisprosessia	V	2,85	1,29	10,2 %	56,9 %
52	1060	Turvallisuuspolitiikan sisältö on koulutettu, tiedotettu ja aina saatavilla	K	2,86	1,17	5,3 %	57,1 %
53	6040	Menetelmä turvapoikkeamien havaitsemiseksi ja suojauksien aloittamiseksi	K	2,89	1,44	15,3 %	57,8 %
54	5060	Johto on sitoutunut turvallisuustavoitteisiin ja jatkuvaan parantamiseen	P	2,90	1,45	16,3 %	58,0 %
55	1051	Lakivaatimukset on täytetty ja henkilötietojen käsittelyprosessit ovat käytössä	P	3,00	1,88	20,4 %	60,0 %
56	3050	Tavoitteissa on huomioidu riskit sekä eri toimintojen ja intressien vaatimukset	K	3,02	1,49	16,0 %	60,3 %
57	7030	Koulutusrekisteri, jolla voidaan osoittaa annettu koulutus ja sen sisältö	V	3,02	1,48	14,3 %	60,4 %
58	1070	Turvallisuuspolitiikka sisältää sitoutumisen jatkuvaan parantamiseen	K	3,02	1,03	4,1 %	60,4 %
59	T2	Turvallisuustyö, asiakirjahallinta ja dokumentaatiot on jaettu ja vastuutettu	P	3,07	1,19	8,8 %	61,4 %
60	7040	Koulutusvaatimus varmistaa, ettei ennen sen täyttymistä aloiteta työtehtävää	V	3,16	1,43	12,2 %	63,3 %
61	5020	Turvallisuusorganisaation roolit ja toimeenpanovalta on koulutettu ja tiedotettu	K	3,21	1,10	3,1 %	64,3 %
62	1050	Turvallisuuspolitiikka huomioi vaatimukset, määräykset, velvoitteet ja lait	K	3,26	1,32	9,7 %	65,2 %
63	1020	Turvallisuuspolitiikan sisältö on riittävän laaja ja kattava	K	3,26	0,98	3,8 %	65,3 %
64	1080	Turvallisuuspolitiikasta löytyy organisaation keskeiset turvallisuustavoitteet	P	3,29	1,19	8,2 %	65,7 %
65	T1	Turvallisuuspolitiikka ohjaa turvallisuustoimintaa, kehittämistä ja raportointia	K	3,31	1,26	9,2 %	66,1 %
66	5040	Turvallisuustyön johtamisesta ja kehittämisestä vastaava henkilö on nimetty	K	3,40	1,01	3,8 %	67,9 %
67	4080	Riskienarviointitulosten mukaan suunnitellaan koulutusvaatimuksia ja -sisältöä	V	3,43	1,24	6,1 %	68,6 %
68	1030	Turvallisuusdokumenteissa on kirjattu perusasiat ja tavoitteet	V	3,47	0,80	0,0 %	69,4 %
69	5050	Turvallisuudesta vastaavalla on riittävät valtuudet tavoitteiden saavuttamiseksi	K	3,63	1,19	0,0 %	72,5 %

PA = KATAKRin mukainen poikkeama-arvion tulos